SRA 6.0
User's Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your system.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2012 Dell Inc.

Trademarks: Dell™, the DELL logo, SonicWALL™, SonicWALL GMS™, SonicWALL ViewPoint™, Aventail™, Reassembly-Free Deep Packet Inspection™, Dynamic Security for the Global Network™, SonicWALL Aventail Advanced End Point Control™ (EPC™), SonicWALL Aventail Advanced Reporting™, SonicWALL Aventail Connect Mobile™, SonicWALL Aventail Connect™, SonicWALL Aventail Native Access Modules™, SonicWALL Aventail Policy Zones™, SonicWALL Aventail Smart Access™, SonicWALL Aventail Unified Policy™, SonicWALL Aventail™ Advanced EPC™, SonicWALL Clean VPN™, SonicWALL Clean Wireless™, SonicWALL Global Response Intelligent Defense (GRID) Network™, SonicWALL Mobile Connect™, SonicWALL SuperMassive™ E10000 Series, and all other SonicWALL product and service names and slogans are trademarks of Dell Inc.

2012 – 11 P/N 232-002121-00 Rev. C

Table of Contents

Chapter 1. Using This Guide 5

About this Guide 5

Organization of this Guide 5

Guide Conventions 6

Current Documentation 6

Quick Access Work Sheet 6

Chapter 2. Virtual Office Overview 7

Virtual Office Overview 7

Accessing Virtual Office Resources 7

Browser Requirements 8

Web Management Interface Overview 10

Certificates 13

Chapter 3. Using Virtual Office Features 15

Importing Certificates 15

Using Two-Factor Authentication 16

User Prerequisites 16

User Configuration Tasks 16

Using One-Time Passwords 20

User Prerequisites 20

User Configuration Tasks 20

Verifying User One-Time Password Configuration 22

Using NetExtender 22

User Prerequisites 22

User Configuration Tasks 24

Installing NetExtender on Android Smartphones 61

Using NetExtender on Android Smartphones 64

Related Documents 77

Using Secure Virtual Assist 77

Understanding Secure Virtual Assist 78

Installing and Launching Secure Virtual Assist 79

Configuring Secure Virtual Assist Settings 80

Selecting a Secure Virtual Assist Mode 82

Launching a Secure Virtual Assist Technician Session 82

Performing Secure Virtual Assist Technician Tasks 83

Initiating a Secure Virtual Assist Session from the Customer View 90

Using Secure Virtual Assist 100

Using Secure Virtual Assist in Unattended Mode 101

Enabling a System for Secure Virtual Access 102

Using the Request Assistance Feature 103

Using Secure Virtual Meeting 104

Features 104

User Roles 104
Coordinator Role 105
Participant Role 117
Using File Shares 119
Using the File Shares Applet 119
Using HTML-Based File Shares 130
Managing Bookmarks 132
Adding Bookmarks 133
Editing Bookmarks 138
Removing Bookmarks 139
Using Bookmarks 139
Using Remote Desktop Bookmarks 139
Using VNC Bookmarks 141
Using FTP Bookmarks 144
Using Telnet Bookmarks 147
Using SSHv1 Bookmarks 147
Using SSHv2 Bookmarks 148
Using Web Bookmarks 149
Using File Share Bookmarks 149
Using Citrix Bookmarks 150
Global Bookmark Single Sign-On Options 155
Per-Bookmark Single Sign-On Options 155
Logging Out of the Virtual Office 157

Appendix A. Support Information 159

Contact Information 159
GNU General Public License (GPL) Source Code 159
Limited Hardware Warranty 159
End User Licensing Agreement 160

Chapter 1

Using This Guide

About this Guide

Welcome to the *Dell SonicWALL SRA User's Guide*. This manual is a user's guide. It provides information on using the Dell SonicWALL SRA user portal called Virtual Office that allows you to create bookmarks and run services over the Dell SonicWALL SRA appliance.

Always check http://www.sonicwall.com/us/Support.html for the latest version of this manual as well as other Dell SonicWALL products and services documentation.

Organization of this Guide

The *Dell SonicWALL SRA User's Guide* organization is structured into the following parts:

Chapter 1 Using this Guide

This chapter provides helpful information for using this guide. It.includes conventions used in this guide, information on how to obtain additional product information, and a Quick Access Worksheet that you should complete before using the SRA appliance.

Chapter 2 Virtual Office Overview

This chapter provides an overview of new Dell SonicWALL SRA appliance user features, NetExtender, File Shares, Secure Virtual Assist, Secure Virtual Access, Secure Virtual Meeting, services, sessions, bookmarks, and service tray menu options.

Chapter 3 Using Virtual Office

This chapter provides procedures on importing certificates, using Two-Factor authentication, using One-Time Passwords, using NetExtender, using Virtual Assist and Virtual Meeting, configuring bookmarks, and using file shares.

Chapter 4 Support Information

This chapter provides the Limited Hardware Warranty, End User Licensing Agreement, and Dell SonicWALL Support contact information.

Guide Conventions

The following conventions used in this guide are as follows:

Convention	Use
Bold	Highlights dialog box, window, and screen names. Also highlights buttons. Also used for file names and text or values you are being instructed to type into the interface.
Italic	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence. Sometimes indicates the first instance of a significant term or concept.

Current Documentation

Check the Dell SonicWALL documentation Web site for the latest versions of all Dell SonicWALL product documentation at http://www.sonicwall.com/us/Support.html

Quick Access Work Sheet

Use the Quick Access Work Sheet to collect important information that you will need and should be completed by your network administrator to allow remote users SSL VPN access.

IP Address:_____

User Name:_____

Password:_____

Domain:_____

Chapter 2

Virtual Office Overview

This chapter provides an overview of the Dell SonicWALL SSL VPN user portal. It also includes an introduction to the SRA appliance and its features and applications. This chapter contains the following sections:

- "Virtual Office Overview" section on page 7
- "Browser Requirements" section on page 8
- "Web Management Interface Overview" section on page 10

Virtual Office Overview

Dell SonicWALL SSL VPN Virtual Office provides secure remote access to network resources, such as applications, files, intranet Web sites, and email through Web access interface such as Microsoft Outlook Web Access (OWA). The underlying protocol used for these sessions is SSL.

With SSL VPN, mobile workers, telecommuters, partners, and customers can access information and applications on your intranet or extranet. What information should be accessible to the user is determined by access policies configured by the Dell SonicWALL SSL VPN administrator.

Accessing Virtual Office Resources

Remote network resources can be accessed in the following ways:

- **Using a standard Web browser** - To access network resources, you must log into the SSL VPN portal. Once authenticated, you may access intranet HTTP and HTTPS sites, offloaded portals, Web-based applications, and Web-based email. In addition, you may upload and download files using FTP or Windows Network File Sharing. All access is performed through a standard Web browser and does not require any client applications to be downloaded to remote users' machines.
- **Using Java thin-client access to corporate desktops and applications** – The Dell SonicWALL SRA security appliance includes several Java or ActiveX thin-client programs that can be launched from within the Dell SonicWALL SRA security appliance. Terminal Services and VNC Java clients allow remote users to access corporate servers and desktops, open files, edit and store data as if they were at the office. Terminal Services provides the ability to open individual applications and support remote sound and print services. In addition, users may access Telnet and SSH servers for SSH version 1 (SSHv1) and SSH version 2 (SSHv2), from the SSL VPN portal.
- **Using the NetExtender SSL VPN client** – The Dell SonicWALL SSL VPN network extension client, NetExtender, is available through the SSL VPN Virtual Office portal via an ActiveX control or through stand-alone applications for Windows, Linux, MacOS, Windows Mobile, and Android smartphone platforms. To connect using the SSL VPN client, log into the portal, download the installer application and then launch the NetExtender connector to establish the SSL VPN tunnel. The NetExtender Android client has a different installation process, described in this guide. Once you have set up the SSL VPN tunnel, you can access network resources as if you were on the local network.

The NetExtender standalone applications are automatically installed on a client system the first time you click on the NetExtender link in the Virtual Office portal. The standalone client can be launched directly from users' computers without requiring them to log in to the SSL VPN portal first.

- **Using the Dell SonicWALL Mobile Connect app** – Dell SonicWALL Mobile Connect is an app for iPhone and iPad that, like NetExtender, uses SSL VPN to enable secure, mobile connections to private networks protected by Dell SonicWALL security appliances. For information about installing and using Dell SonicWALL Mobile Connect, see the *Dell SonicWALL Mobile Connect User's Guide* available on www.sonicwall.com, at: http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=PG&id=482

For SSL VPN to work as described in this guide, the SonicWALL SRA security appliance must be installed and configured according to the directions provided in the *SonicWALL SRA Getting Started Guide* for your model.

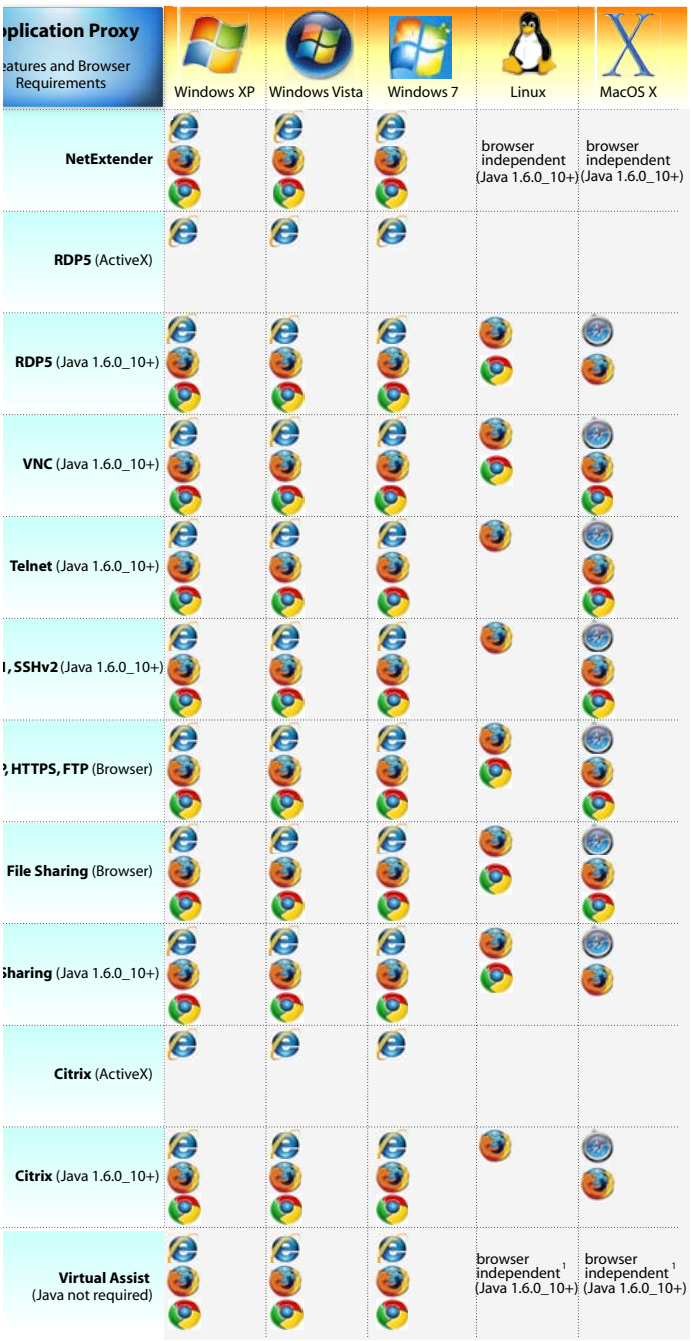
Browser Requirements

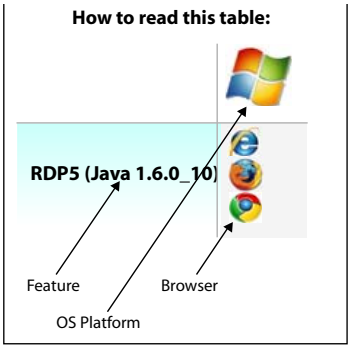
The following Web browsers are supported for the SSL VPN Virtual Office portal:

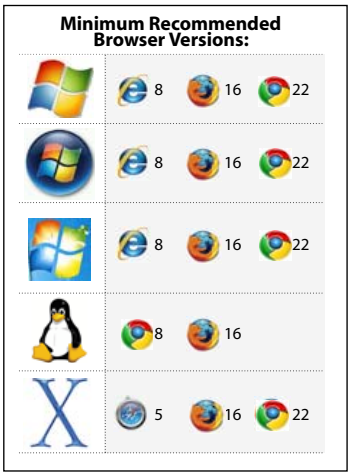
- Internet Explorer 8.0+, 9.0+
- Firefox 16.0+
- Safari 5.0+
- Chrome 22.0+

For administrator management interface Web browser compatibility, refer to the *SonicWALL SSL VPN Administrator's Guide*.

The following table provides specific browser requirements.







Notes:

1 MacOS and Linux supports Virtual Assist on the client-side only. Technician must be running a supported version of Windows operating system.

To configure SonicOS SSL VPN firmware, an administrator must use a Web browser with JavaScript, cookies, and SSL enabled.

Virtual Assist is fully supported on Windows platforms. Virtual Assist is certified to work on Windows 7, Windows Vista and Windows XP. Limited functionality is supported on Mac OS where customers can request for assistance via web-requests.

Web Management Interface Overview

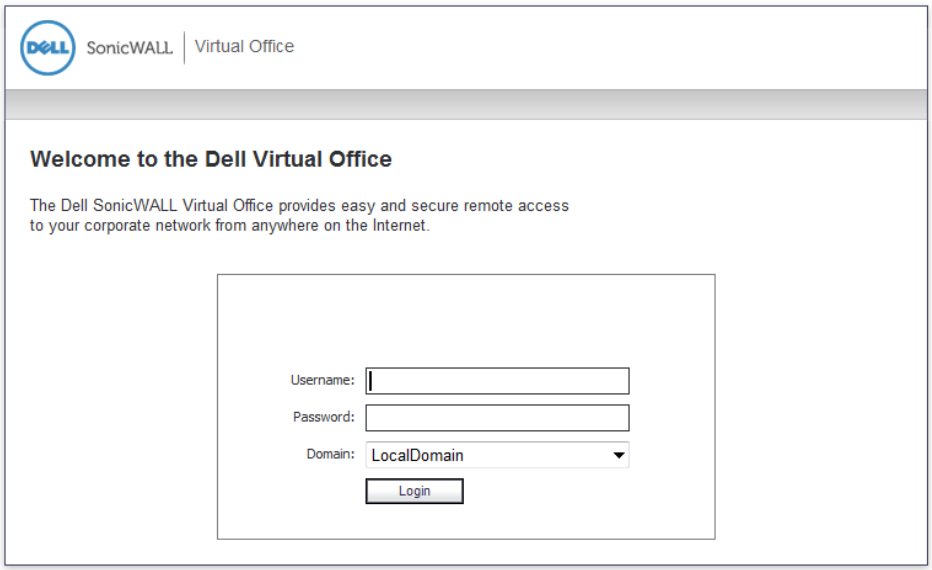
From your workstation at your remote location, launch an approved Web browser and browse to your SRA appliance at the URL provided to you by your network administrator.

Step 1 Open a Web browser and enter **https://192.168.200.1** (the default LAN management IP address) in the **Location** or **Address** field.

Step 2 A security warning may appear. Click the **Yes** button to continue.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

Step 3 The **SonicWALL SSL VPN Management Interface** displays and prompts you to enter your user name and password. As a default value, enter **admin** in the **User Name** field, **password** in the **Password** field, and select a domain from the **Domain** drop-down list and click the **Login** button. Only **LocalDomain** allows administrator privileges. Note that your administrator may have set up another login and password for you that has only user privileges.

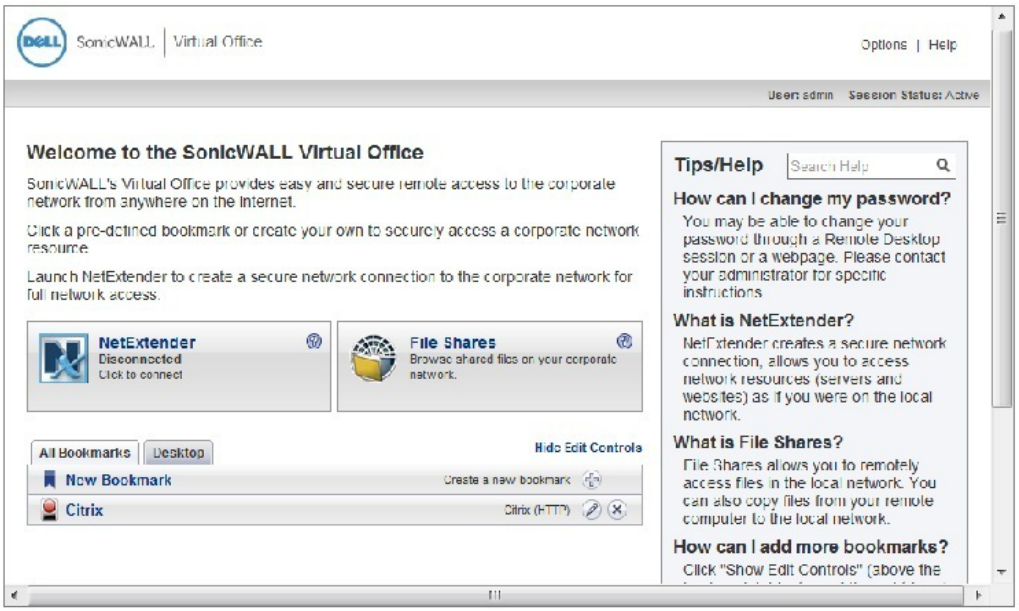


The default page displayed is the Virtual Office home page. The default version of this page shows a SonicWALL logo, although your company's system administrator may have customized this page to contain a logo and look and feel of your company. Go to the Virtual Office Overview, page 7 to learn more about the Virtual Office home page.

From the Virtual Office portal home page, you cannot navigate to the administrator's environment. If you have administrator's privileges and want to enter the administrator environment, you need to go back to the login page and enter a username and password that

have administrator privileges, and login again using the LocalDomain domain. Only the LocalDomain allows administrator access to the management interface. Also note that the domain is independent of the privileges set up for the user.

Logging in as a user takes you directly to Virtual Office. The Virtual Office Home page displays as shown here.


SonicWALL | Virtual Office
Options | Help
User: admin Session Status: Active
Welcome to the SonicWALL Virtual Office
SonicWALL's Virtual Office provides easy and secure remote access to the corporate network from anywhere on the Internet.
Click a pre-defined bookmark or create your own to securely access a corporate network resource.
Launch NetExtender to create a secure network connection to the corporate network for full network access.
NetExtender
Disconnected
Click to connect
File Shares
Browse shared files on your corporate network.
All Bookmarks
Desktop
Hide Edit Controls
New Bookmark
Create a new bookmark
Citrix
Citrix (HTTP)
Tips/Help
Search Help
How can I change my password?
You may be able to change your password through a Remote Desktop session or a webpage. Please contact your administrator for specific instructions.
What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local network.
What is File Shares?
File Shares allows you to remotely access files in the local network. You can also copy files from your remote computer to the local network.
How can I add more bookmarks?
Click "Show Edit Controls" (above the

The Virtual Office content will vary based on the configuration of your network administrator. Some bookmarks and services described in the *SonicWALL SSL VPN User's Guide* may not be displayed when you log into the SonicWALL SRA security appliance.

The Virtual Office consists of the nodes described in the following table.

Node	Description
File Shares	Provides access to the File Shares utility, which gives remote users with a secure Web interface access to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.
NetExtender	Provides access to the NetExtender utility, a transparent SSL VPN client for Windows, MacOS, Linux, Windows Mobile, or Android smartphone users that allows you to run any application securely on the remote network. It acts as an IP-level mechanism provided by the virtual interface that negotiates the ActiveX component (on Windows with IE), using a Point-to-Point Protocol (PPP) adapter instance. On non-Windows platforms except Android, Java controls are used to automatically install NetExtender from the Virtual Office portal. After installation, NetExtender automatically launches and connects a virtual adapter for SSL secure NetExtender point-to-point access to permitted hosts and subnets on the internal network.

Node	Description
Secure Virtual Assist	Provides access to Virtual Assist, an easy to use tool that allows SonicWALL SSL VPN users to remotely support customers by taking control of their computers while the customer observes. Virtual Assist is a lightweight, thin client that installs automatically using Java from the SonicWALL SSL VPN Virtual Office without requiring the installation of any external software. For computers that do not support Java, Virtual Assist can be manually installed by downloading an executable file from the Virtual Office.
Secure Virtual Meeting	Provides access to Virtual Meeting, which allows multiple users to view a desktop and interactively participate in a meeting from virtually anywhere with an Internet connection. Virtual Meeting is similar to the one-to-one desktop sharing provided by Virtual Assist except multiple users can share a desktop.
Secure Virtual Access (if configured by administrator	Secure Virtual Access allows technicians to gain access to systems outside the LAN of the SRA appliance. After downloading and installing the thin client for Secure Virtual Access mode, the system will appear only on that technician's Virtual Assist support queue, within the SRA's management interface.
Bookmarks	Provides a list of available bookmarks which are objects that enable you to connect to a location or application conveniently and quickly.
Options	Provides the option to change user password and use single sign-on, if enabled by the administrator.
Online Help	Launches online help for Virtual Office.
Tips/Help	Provides a short list of common questions and tips about the Virtual Office.
Logout	Logs you out of the Virtual Office environment.

The Home page provides customized content and links to network resources. The Home Page may contain support contact information, VPN instructions, company news, or technical updates.

Only a Web browser is required to access intranet Web sites, File Shares, and FTP sites. VNC, Telnet and SSHv1 require Java. SSHv2 provides stronger encryption than SSHv1, requires SUN JRE 1.4 or above and can only connect to servers that support SSHv2. Terminal Services requires either Java or ActiveX on the client machine.

As examples of tasks you can perform and environments you can reach through Virtual Office, you can connect to:

- Intranet Web or HTTPS sites – If your organization supports Web-based email, such as Outlook Web Access, you can also access Web-based email
- The entire network by launching the NetExtender client
- FTP servers for uploading and downloading files
- The corporate network neighborhood for file sharing
- Telnet and SSH servers
- Desktops and desktop applications using Terminal Services or VNC.
- Email servers via the NetExtender client.

The administrator determines what resources are available to users from the SonicWALL SSL VPN Virtual Office. The administrator can create user, group, and global policies that disable access to certain machines or applications on the corporate network.

The administrator may also define bookmarks, or preconfigured links, to Web sites or computers on the intranet. Additional bookmarks may be defined by the end user.

SonicWALL NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

Certificates

If the SRA appliance uses a self-signed SSL certificate for HTTPS authentication, then it is recommended to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWALL recommends that you import the certificate. The easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page.

If the certificate is not issued by an authorized organization, a message is displayed warning users of the risk. A user can then view detailed information and choose to continue or end the connection.

Chapter 3

Using Virtual Office Features

This chapter provides details on how to use the features in the Dell SonicWALL SSL VPN user portal, including NetExtender, configuring bookmarks, accessing services, and using file shares. This chapter contains the following sections:

- "Importing Certificates" section on page 15
- "Using Two-Factor Authentication" section on page 16
- "Using One-Time Passwords" section on page 20
- "Using NetExtender" section on page 22
- "Using Secure Virtual Assist" section on page 77
- "Using Secure Virtual Meeting" section on page 104
- "Using File Shares" section on page 119
- "Managing Bookmarks" section on page 132
- "Using Bookmarks" section on page 139
- "Logging Out of the Virtual Office" section on page 157

Importing Certificates

If the SSL VPN gateway uses a self-signed SSL certificate for HTTPS authentication, then it is recommended to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, Dell SonicWALL recommends that you import the certificate.

If using Internet Explorer, the easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page. The following warning messages may be displayed:

Potential Scripting Violation
This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
Yes
No

Click **Yes**. The certificate will be imported.

Note Certificates can only be imported through this method if you are using Internet Explorer. Certificates for other browsers such as Chrome or Firefox must be imported manually.

Using Two-Factor Authentication

The following sections describe how to log in to the SSL VPN Virtual Office portal using two-factor authentication:

- "User Prerequisites" on page 16
- "User Configuration Tasks" on page 16

User Prerequisites

Before you can log in using two-factor authentication, you must meet the following prerequisites:

- Your administrator has created your user account.
- You have an account with a two-factor authentication server that conforms to the RFC standard.

User Configuration Tasks

The following sections describe how users log in to the Dell SonicWALL SRA appliance using the two types of two-factor authentication:

- "RSA Two-Factor User Authentication Process" on page 16
- "VASCO Two-Factor User Authentication Process" on page 18
- "Other RADIUS Server Two-Factor Authentication Process" on page 19

RSA Two-Factor User Authentication Process

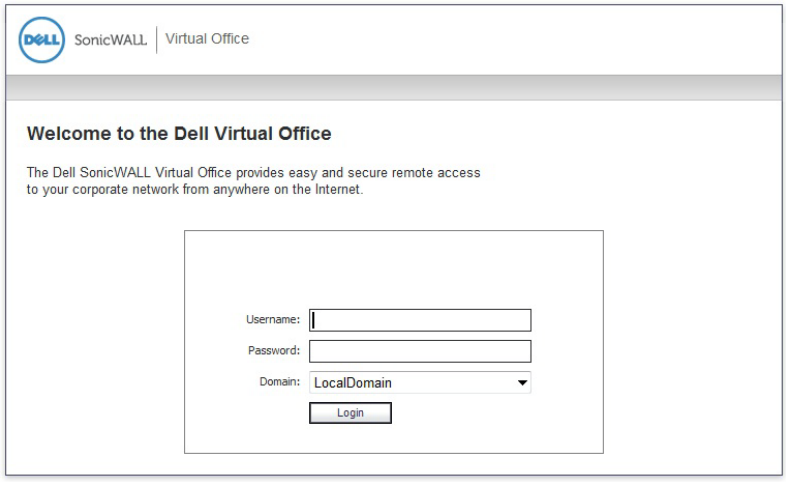
The following sections describe user tasks when using RSA two-factor authentication to log in to the Dell SonicWALL SSL VPN Virtual Office:

- "Logging into the SSL VPN Virtual Office Using RSA Two-Factor Authentication" on page 16
- "Creating a New PIN" on page 17
- "Waiting for the Next Token Mode" on page 18

Logging into the SSL VPN Virtual Office Using RSA Two-Factor Authentication

To log in to the Dell SonicWALL SSL VPN Virtual Office using RSA two-factor authentication, perform the following steps.

Step 1 Enter the IP address of the SRA appliance in your computers browser. The authentication window is displayed.



Step 2 Enter your username in the **Username** field.

Step 3 The first time you log in to the Virtual office, your entry in the password field depends on whether your system requires a PIN:

- If you already have a PIN, enter the passcode in the **Password** field. The passcode is the user PIN and the SecurID token code. For example, if the user's PIN is 8675 and the token code is 30966673, then the passcode is 867530966673.
- If a PIN is required, but you do not yet have a PIN, enter the SecurID token code in the **Password** field. You will be prompted to create a PIN.
- If the RSA server does not require a PIN, simply enter the SecurID token code.

Note Consult with your network administrator to determine if your configuration requires a PIN.

Step 4 Select the appropriate **Domain**. If manually entering the Domain, it is case-sensitive.

Step 5 Click **Login**.

Creating a New PIN

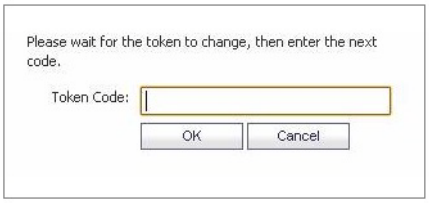
The RSA Authentication Manager automatically determines when users are required to create a new PIN. will determines that user associated with a particular token requires a new PIN. The SRA appliance prompts the user to enter new PIN.

Enter the PIN in the **New PIN** field and again in the **Confirm PIN** field and click **OK**. The PIN must be between 4 and 8 characters long.

Step 6 The RSA Authentication Manager verifies that the new PIN is an acceptable PIN. If the PIN is accepted, the user is prompted to log in with the new passcode.

Waiting for the Next Token Mode

If user authentication fails three consecutive times, the RSA server requires the user to generate and enter a new token. To complete authentication, the user is prompted to wait for the token to change and enter the next token.



VASCO Two-Factor User Authentication Process

The following sections describe user tasks when using RSA two-factor authentication:

- “Logging into the SSL VPN Virtual Office Using VASCO Two-Factor Authentication” on page 18
- “Creating a New PIN” on page 17

Logging into the SSL VPN Virtual Office Using VASCO Two-Factor Authentication

To log in to the Dell SonicWALL SSL VPN Virtual Office using VASCO two-factor authentication, perform the following steps:

Step 1 Enter the IP address of the SRA appliance in your computer's browser. The authentication window is displayed.

Step 2 Enter your username in the **Username** field.

Step 3 Enter the passcode in the **Password** field. Your entry in the password field depends on whether your system requires a PIN:

- If you already have a PIN, enter the passcode in the **Password** field. The passcode is the user PIN and the VASCO Digipass token code. For example, if the user's PIN is 8675 and the token code is 30966673, then the passcode is 867530966673.
- If a PIN is required, but you do not yet have a PIN, enter the VASCO Digipass code in the **Password** field. You will be prompted to create a PIN.
- If the RSA server does not require a PIN, simply enter the VASCO Digipass code.

Note Consult with your network administrator to determine if your configuration requires a PIN.

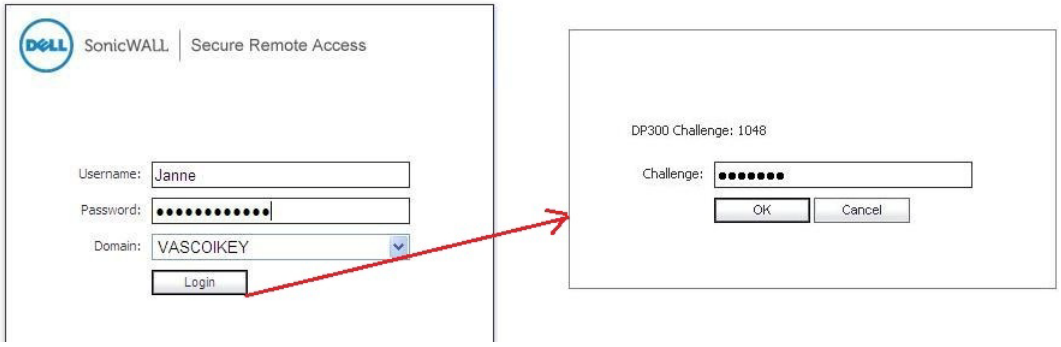
Step 4 Select the appropriate **Domain**. If manually entering the Domain, it is case-sensitive.

Step 5 Click **Login**.

Other RADIUS Server Two-Factor Authentication Process

To log in to the Virtual Office using another type of RADIUS server for two-factor authentication, perform the following steps:

Step 1 Enter the IP address of the SRA appliance in your computers browser. The authentication window is displayed.



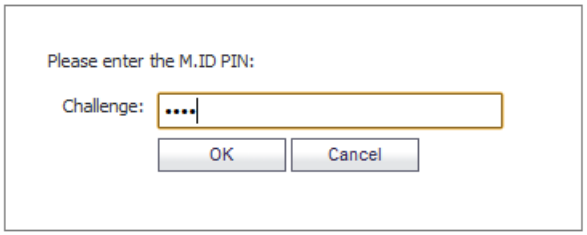
Step 2 Enter your username in the **Username** field.

Step 3 Enter your password in the **Password** field.

Step 4 Select the appropriate **Domain**. If manually entering the Domain, it is case-sensitive.

Step 5 Click **Login**.

Step 6 You will be prompted to enter additional information, the details of which will depend on the type of RADIUS server used. The example below shows an M.ID RADIUS server, which first prompts you to "Please enter the M.ID PIN." Enter the PIN in the **Challenge** field and click **OK**.



Step 7 You will then be prompted to “Please enter the M.ID Passcode.” Enter the passcode received through email or text message in the **Challenge** field and click **OK**.

Using One-Time Passwords

The following sections describe how to use one-time passwords:

- User Prerequisites, page 20
- User Configuration Tasks, page 20
- Verifying User One-Time Password Configuration, page 22
- Using NetExtender, page 22

User Prerequisites

Users must have a user account enabled in the SSL VPN management interface. Only users enabled by the administrator to use the One-Time Password feature will need to perform the following configuration tasks. The administrator must enable a correct email address that is accessible by the user. Users cannot enable the One-Time Password feature and they must be able to access the SSL VPN Virtual Office portal.

User Configuration Tasks

To use the One-Time Password feature, perform the following steps:

Step 1 If you are not logged into the SSL VPN Virtual Office user interface, open a Web browser and type the Virtual Office interface URL in the **Location** or **Address** bar and press **Enter**. Type in your user name in the **User Name** field and your password in the **Password** field, then select the appropriate domain from the **Domain** drop-down menu. Click **Login**.

Step 2 The prompt “A temporary password has been sent to user@email.com” will appear, displaying your pre-configured email account.

Step 3 Login to your email account to retrieve the one-time password.

Step 4 Type or paste the one-time password into the **Password:** field where prompted and click **Login**.

Step 5 You will be logged in to the Virtual Office.

Note One-time passwords are immediately deleted after a successful login, and cannot be used again. Unused one-time passwords will expire according to each user’s timeout policy.

Configuring One-Time Passwords for SMS-Capable Phones

One-Time Passwords can be configured to be sent via email directly to SMS-capable phones. Contact your cell phone service provider for further information about enabling SMS.

Below is a list of SMS email formats for selected major carriers, where 4085551212 represents a 10-digit telephone number and area code.

Note These SMS email formats are for reference only. These email formats are subject to change and may vary. You may need additional service or information from your provider before using SMS. Contact the SMS provider directly to verify these formats and for further information on SMS services, options, and capabilities.

- Verizon: 4085551212@vtext.com
- Sprint: 4085551212@messaging.sprintpcs.com
- AT&T: 4085551212@mobile.att.net
- Cingular: 4085551212@mobile.mycingular.com
- T-Mobile: 4085551212@tmomail.net
- Nextel: 4085551212@messaging.nextel.com
- Virgin Mobile: 4085551212@vmobl.com
- Qwest: 4085551212@qwestmp.com

For a more complete list, see the *Dell SonicWALL SSL VPN Administrator's Guide*.

Verifying User One-Time Password Configuration

If you are successfully logged in to Virtual Office, you have correctly used the One-Time Password feature.

If you cannot login using the One-Time Password feature, verify the following:

- Are you able to login to the Virtual Office without being prompted to check your email for a one-time password? You have not been enabled to use the One-Time Password feature. Contact your SSL VPN administrator.
- Is your email address correct? If your email address has been entered incorrectly, contact your SSL VPN administrator to correct it.
- Is there no email with a one-time password? Wait a few minutes and refresh your email inbox. Check your spam filter. If there is no email after several minutes, try to login again to generate a new one-time password.
- Have you accurately typed the one-time password in the correct field? Re-type or copy and paste the one-time password.

Using NetExtender

The following sections describe how to use Dell SonicWALL NetExtender:

- "User Prerequisites" section on page 22
- "User Configuration Tasks" section on page 24
- "Verifying NetExtender Operation from the System Tray" section on page 46

User Prerequisites

Prerequisites for Windows Clients:

Windows clients must meet the following prerequisites in order to use NetExtender:

- One of the following platforms:
  - Windows 7 Services Pack 1
  - Windows Vista Service Pack 2 (32-bit & 64-bit)
  - Windows XP Home or Professional, Windows XP Service Pack 3
- One of the following browsers:
  - Internet Explorer 8.0 and higher
  - Mozilla Firefox 16.0 and higher
  - Google Chrome 22.0 and higher
- To initially install the NetExtender client, the user must be logged in to the PC with administrative privileges.
- Downloading and running scripted ActiveX files must be enabled on Internet Explorer.
- If the SSL VPN gateway uses a self-signed SSL certificate for HTTPS authentication, then it is necessary to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate

Authority, Dell SonicWALL recommends that you import the certificate. The easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page.

Prerequisites for Windows Mobile Clients

NetExtender supports the following Windows Mobile platforms:

- Windows Mobile 5 PocketPC version
- Windows Mobile 6 Professional/Classic version

Windows Mobile 5 Smart Phone version and Windows Mobile 6 Standard version are not currently supported.

Prerequisites for MacOS Clients:

MacOS clients meet the following prerequisites in order to use NetExtender:

- MacOS 10.5 and higher
- Java 1.5 and higher
- Both PowerPC and Intel Macs are supported.

Prerequisites for Linux Clients:

Linux 32-bit or 64-bit clients are supported for NetExtender when running one of the following distributions (32-bit or 64-bit):

- Linux Fedora Core 15 or higher, Ubuntu 11.10 or higher, or OpenSUSE 10.3 or higher
- Java 1.5 and higher is required for using the NetExtender GUI.

The NetExtender client has been known to work on other distributions as well, but these are not officially supported.

Note Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Java 1.5 or higher, you can use the command-line interface version of NetExtender.

Prerequisites for Apple iOS Clients

Dell SonicWALL Mobile Connect is supported on Apple iPhone, iPad, and iPod Touch devices running Apple iOS:

- iPhone 4S – running Apple iOS 5 or higher
- iPhone 4 – running Apple iOS 4.2 or higher
- iPhone 3GS – running Apple iOS 4.2 or higher
- iPhone 3G – running Apple iOS 4.2 or higher
- iPad 3 – running Apple iOS 4.2 or higher
- iPad 2 – running Apple iOS 4.2 or higher
- iPad – running Apple iOS 4.2 or higher
- iPod Touch (2nd Generation or later) – running Apple iOS 4.2 or higher

Mobile Connect acts as a NetExtender client when connecting to the Dell SonicWALL SRA. For Mobile Connect access to succeed, the portal must be set to allow NetExtender connections and the user account and group must be authorized to use NetExtender.

Dell SonicWALL Mobile Connect is an app for iPhone and iPad that, like NetExtender, uses SSL VPN to enable secure, mobile connections to private networks protected by Dell SonicWALL security appliances. For information about installing and using Dell SonicWALL Mobile Connect, see the *Dell SonicWALL Mobile Connect User's Guide* at:
http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=PG&id=482

Mobile Connect is compatible with SRA and is a free download from iOS and Adroid (4.0+) app stores.

Prerequisites for Android Smartphone Clients

The NetExtender Android client is supported on rooted smartphones running the following versions of the Android operating system:

- 1.6 or higher

  The NetExtender Android client is compatible with any Dell SonicWALL SSL VPN firmware version that supports the NetExtender Linux client, specifically:
- SSL VPN 4.0 and higher

  As new features are added, users must install the updated client to access all the features supported by the new firmware. Likewise, if a new client is used with older firmware, some client features may not be functional. For best results, the latest firmware should always be used with the latest client.

Note Only rooted devices are supported for NetExtender Android in Dell SonicWALL SSL VPN.
The rooting requirement is due to limitations and restrictions of the Android platform. A layer 3 VPN client like NetExtender requires root permission for certain necessary OS level operations.

Warning **Rooting your phone may void your warranty. Consult your contract or User's Guide, or call your service provider for more information.**

Alternatively, the Dell SonicWALL Mobile Connect client can be used for smartphones running Android version 4.0 or higher.

User Configuration Tasks

Dell SonicWALL NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

The following sections describe how to use NetExtender on the various supported platforms:

Windows Platform Installation

- "Installing NetExtender Using the Mozilla Firefox Browser" section on page 25
- "Installing NetExtender Using the Internet Explorer Browser" section on page 27
-

Windows Platform Usage

- “Launching NetExtender Directly from Your Computer” section on page 32
- “Configuring NetExtender Properties” section on page 33
- “Configuring NetExtender Connection Scripts” section on page 36
- “Configuring Proxy Settings” section on page 38
- “Configuring NetExtender Log Properties” section on page 39
- “Disconnecting NetExtender” section on page 43
- “Upgrading NetExtender” section on page 44
- “Authentication Methods” section on page 44
- “Verifying NetExtender Operation from the System Tray” section on page 46
- “Using the NetExtender Command Line Interface” section on page 47

MacOS Platform

- “Installing NetExtender on MacOS” section on page 48
- “Using NetExtender on MacOS” section on page 50

Linux Platform

- “Installing NetExtender on Linux” section on page 52
- “Using NetExtender on Linux” section on page 54

Windows Mobile Platform

- “Installing and Using NetExtender for Windows Mobile” section on page 57

Android Smartphone Platform

- “Installing NetExtender on Android Smartphones” section on page 61
- “Using NetExtender on Android Smartphones” section on page 64

Installing NetExtender Using the Mozilla Firefox Browser

To use NetExtender for the first time using the Chrome browser, perform the following:

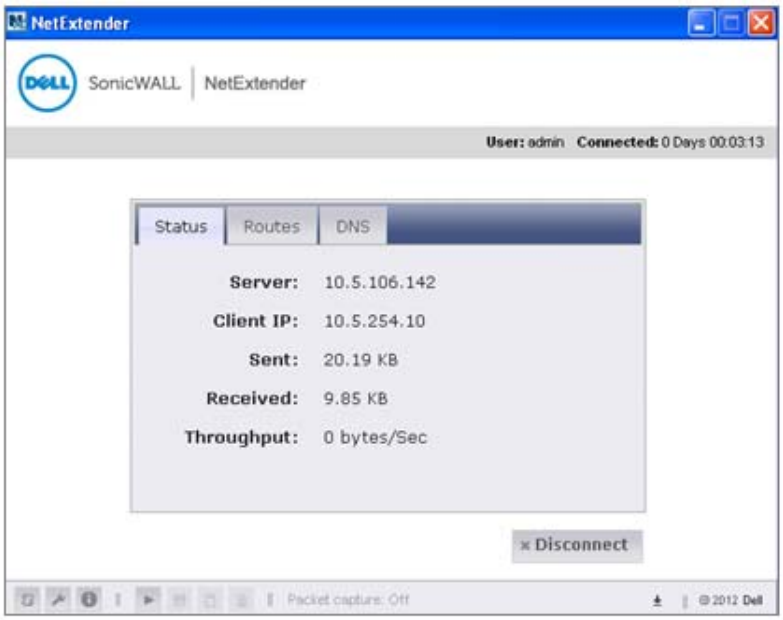
Step 1 To launch NetExtender, first log in to the SSL VPN portal.

Step 2 Click the **NetExtender** button.

The first time you launch NetExtender, it will automatically add a plug-in to Chrome extension.

Step 3 Return to the SSL VPN portal and click on the NetExtender button. The portal will automatically install the NetExtender stand-alone application on your computer. If an older version of NetExtender is installed on the computer, the NetExtender launcher removes the old version and installs the new version

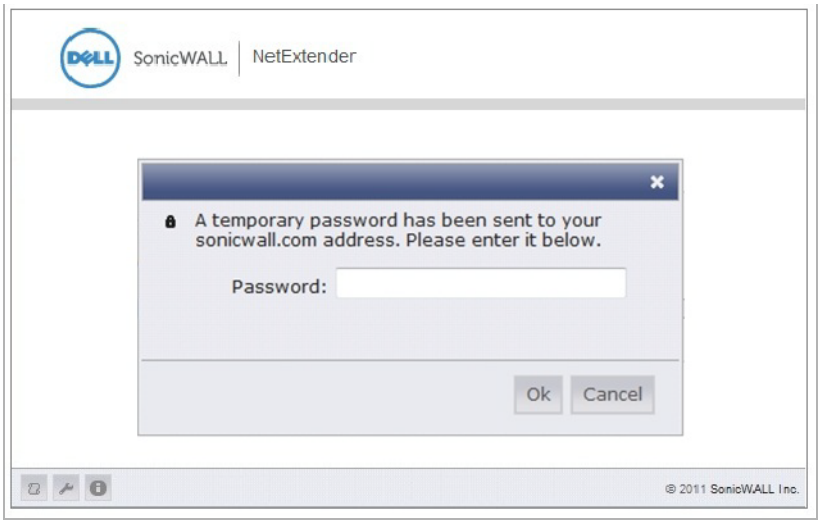
Step 4 When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.



The Status tab provides the following information:

Field	Description
Server	Indicates the name of the server to which the NetExtender client is connected.
Client IP	Indicates the IP address assigned to the NetExtender client.
Sent	Indicates the amount of traffic the NetExtender client has transmitted since initial connection.

Field	Description
Received	Indicates the amount of traffic the NetExtender client has received since initial connection.
Throughput	Indicates the current NetExtender throughput rate.



Closing the window (clicking on the **x** icon in the upper right corner of the window) will not close the NetExtender session, but will minimize it to the system tray for continued operation. Additionally, a balloon icon in the system tray appears, indicating NetExtender has successfully installed.

Step 5 The NetExtender icon is displayed in the task bar.

Installing NetExtender Using the Internet Explorer Browser

Dell SonicWALL SSL VPN NetExtender is fully compatible with Microsoft Windows 7 32-bit and 64-bit, and supports the same functionality as with other Windows operating systems. NetExtender is also compatible with the Mac OS X Lion 10.7.

Note It may be necessary to restart your computer when installing NetExtender on Windows Vista or Windows 7.

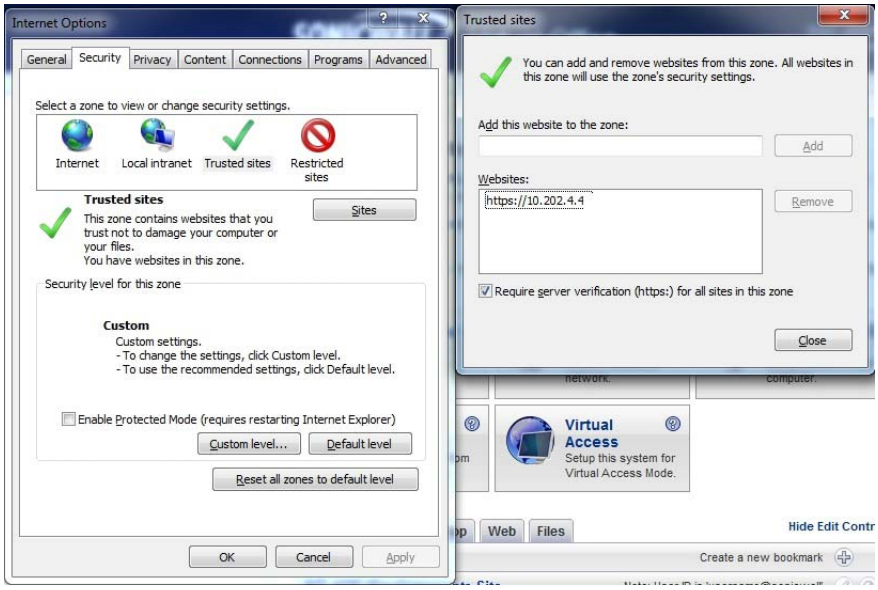
Internet Explorer Prerequisites

It is recommended that you add the URL or domain name of your SSL VPN server to Internet Explorer's trusted sites list. This will simplify the process of installing NetExtender and logging in, by reducing the number of security warnings you will receive. To add a site to Internet Explorer's trusted sites list, complete the following procedure:

Step 1 In Internet Explorer, go to **Tools > Internet Options**.

Step 2 Click on the **Security** tab.

Step 3 Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.



Step 4 Enter the URL or domain name of your SSL VPN server in the **Add this Web site to the zone** field and click **Add**.

Step 5 Click **Ok** in the **Trusted Sites** and **Internet Options** windows.

Installing NetExtender from Internet Explorer

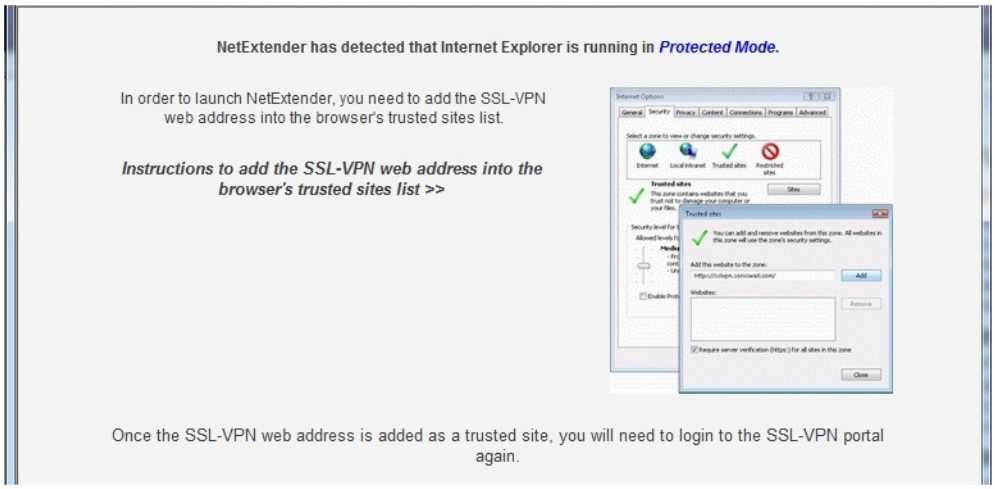
To install and launch NetExtender for the first time using the Internet Explorer browser, perform the following:

Step 1 Log in to the SSL VPN Virtual Office portal.

Step 2 Click the **NetExtender** button.

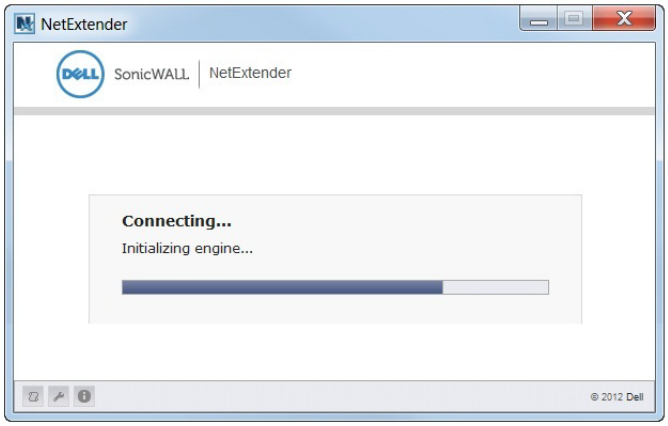
Step 3 A User Account Control window may appear asking "Do you want to allow this program to make changes to this computer?" Click **Yes**.

Step 4 The first time you launch NetExtender, you must first add the SSL VPN portal to your list of trusted sites. If you have not done so, the follow message will display.


NetExtender has detected that Internet Explorer is running in Protected Mode.
In order to launch NetExtender, you need to add the SSL-VPN web address into the browser's trusted sites list.
Instructions to add the SSL-VPN web address into the browser's trusted sites list >>
Once the SSL-VPN web address is added as a trusted site, you will need to login to the SSL-VPN portal again.

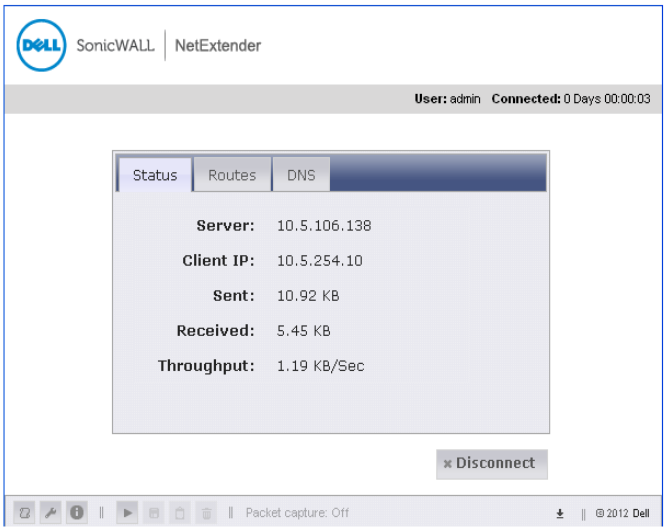
Step 5 For details on how to add the Virtual Office as a trusted site, see the "Internet Explorer Prerequisites" section on page 28.

Step 6 Return to the SSL VPN portal and click on the **NetExtender** button. The portal will automatically install the NetExtender stand-alone application on your computer. The NetExtender installer window opens.



Step 7 If an older version of NetExtender is installed on the computer, the NetExtender launcher will remove the old version and then install the new version.

Step 8 When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.



Installing NetExtender Using the Chrome Browser

Dell SonicWALL SSL VPN NetExtender is fully compatible with Microsoft Windows 7 32-bit and 64-bit, and supports the same functionality as with other Windows operating systems. NetExtender is also compatible with the Mac OS X Lion 10.7.

Note It may be necessary to restart your computer when installing NetExtender on Windows Vista or Windows 7.

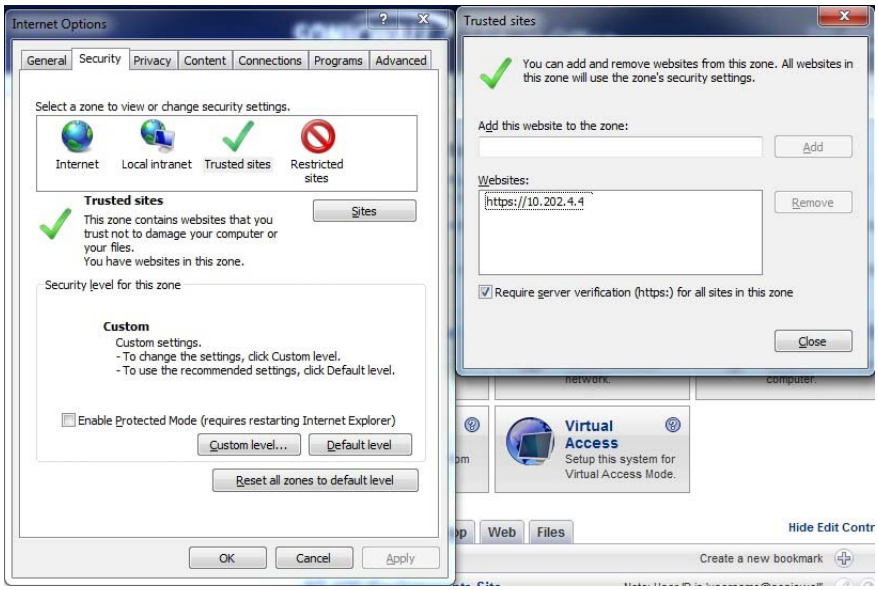
Internet Explorer Prerequisites

It is recommended that you add the URL or domain name of your SSL VPN server to Chrome's trusted sites list. This will simplify the process of installing NetExtender and logging in, by reducing the number of security warnings you will receive. To add a site to Chrome's trusted sites list, complete the following procedure:

Step 1 In Internet Explorer, go to **Tools > Internet Options**.

Step 2 Click on the **Security** tab.

Step 3 Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.



Step 4 Enter the URL or domain name of your SSL VPN server in the **Add this Web site to the zone** field and click **Add**.

Step 5 Click **Ok** in the **Trusted Sites** and **Internet Options** windows.

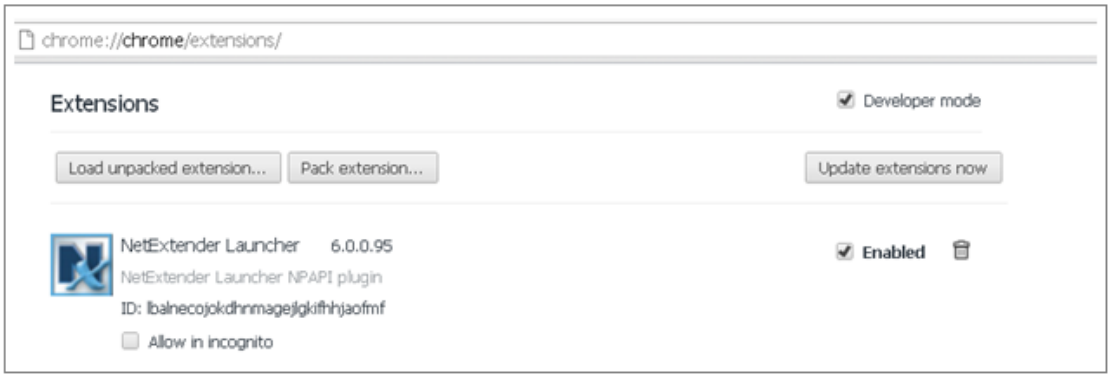
Installing NetExtender from Internet Explorer

To install and launch NetExtender for the first time using the Chrome browser, perform the following:

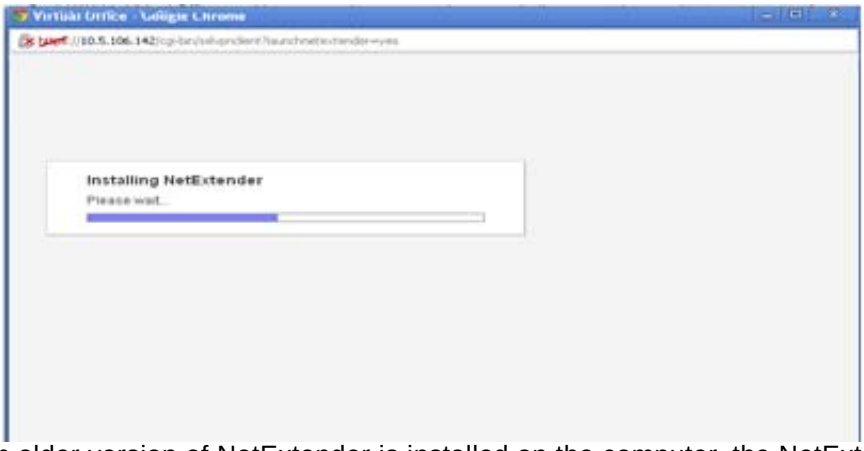
Step 1 Log in to the SSL VPN Virtual Office portal.

Step 2 Click the **NetExtender** button.

Step 3 Pull the NetExtender plug-in to Chrome Extensions.

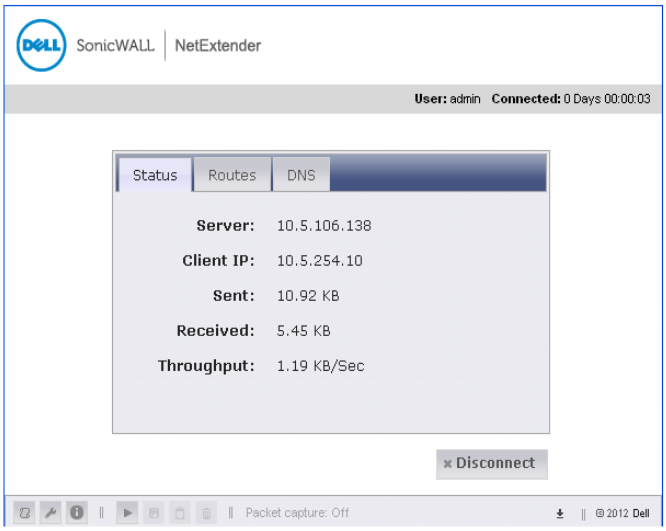


Step 4 Return to the SSL VPN portal and click on the **NetExtender** button. The portal will automatically install the NetExtender stand-alone application on your computer. The NetExtender installer window opens.



If an older version of NetExtender is installed on the computer, the NetExtender launcher will remove the old version and then install the new version.

Step 5 When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.



Launching NetExtender Directly from Your Computer

After the first access and installation of NetExtender, you can launch NetExtender directly from your computer without first navigating to the SSL VPN portal. To launch NetExtender, complete the following procedure:

Step 1 Navigate to **Start > All Programs**.

Step 2 Select the **Dell SonicWALL NetExtender** folder, and then click on **SonicWALL NetExtender**. The NetExtender login window is displayed.

Step 3 The IP address of the last SSL VPN server you connected to is displayed in the **SSL VPN Server** field. To display a list of recent SSL VPN servers you have connected to, click on the arrow.

Step 4 Enter your username and password.

Step 5 The last domain you connected to is displayed in the **Domain** field.

Note The NetExtender client will report an error message if the provided domain is invalid when you attempt to connect. Please keep in mind that domain names are case-sensitive.

Step 6 The drop-down menu at the bottom of the window provides three options for remembering your username and password:

- Save user name & password if server allows
- Save user name only if server allows
- Always ask for user name & password

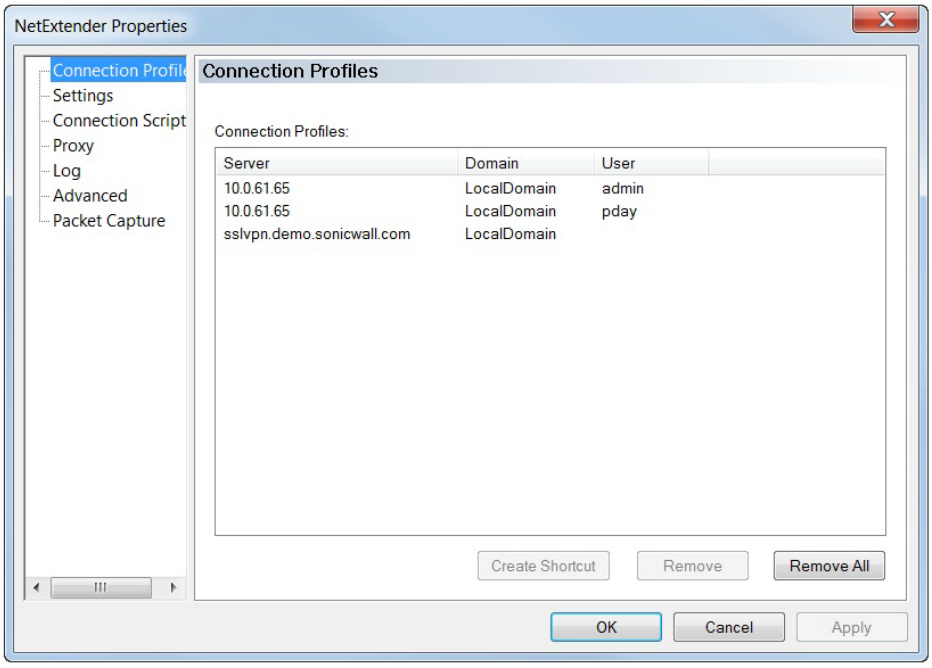
Tip Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

Configuring NetExtender Properties

Complete the following procedure to configure NetExtender properties:

Step 1 Right click on the icon in the system tray and click on **Properties...** The NetExtender Properties window is displayed.

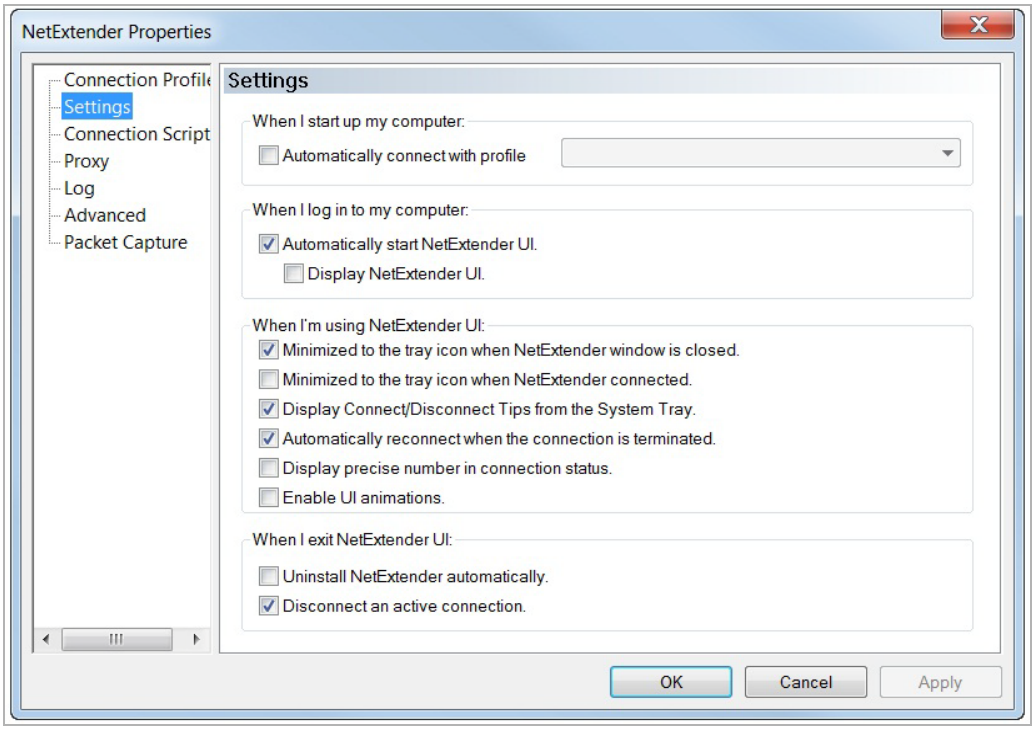
Step 2 The **Connection Profiles** tab displays the SSL VPN connection profiles you have used, including the IP address of the SSL VPN server, the domain, and the username.


NetExtender Properties
Connection Profil
Settings
Connection Script
Proxy
Log
Advanced
Packet Capture
Connection Profiles
Connection Profiles:
Server
Domain
User
10.0.61.65
LocalDomain
admin
10.0.61.65
LocalDomain
pday
sslvpn.demo.sonicwall.com
LocalDomain
Create Shortcut
Remove
Remove All
OK
Cancel
Apply

Step 3 To create a shortcut on your desktop that will launch NetExtender with the specified profile, highlight the profile and click **Create Shortcut**.

Step 4 To delete a profile, highlight it by clicking on it and then click the **Remove** buttons. Click the **Remove All** buttons to delete all connection profiles.

Step 5 The **Settings** tab allows you to customize the behavior of NetExtender.



Step 6 To have NetExtender launch when you log in to your computer, check the **Automatically start NetExtender UI**. NetExtender will start, but will only be displayed in the system tray. To have the NetExtender log-in window display, check the **Display NetExtender UI** check box.

Step 7 Select **Minimize to the tray icon when NetExtender window is closed** to have the NetExtender icon display in the system tray. If this option is not checked, you will only be able to access the NetExtender UI through Window's program menu.

Step 8 Select **Display Connect/Disconnect Tips from the System Tray** to have NetExtender display tips when you mouse over the NetExtender icon.

Step 9 Select **Automatically reconnect when the connection is terminated** to have NetExtender attempt to reconnect when it loses connection.

Step 10 Select **Display precise number in connection status** to display precise byte value information in the connection status.

Step 11 Select the **Enable UI animations** check box to enable the sliding animation effects in the UI.

Step 12 Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

Step 13 Select **Disconnect an active connection** to have NetExtender log out of all of your SSL VPN sessions when you exit a NetExtender session

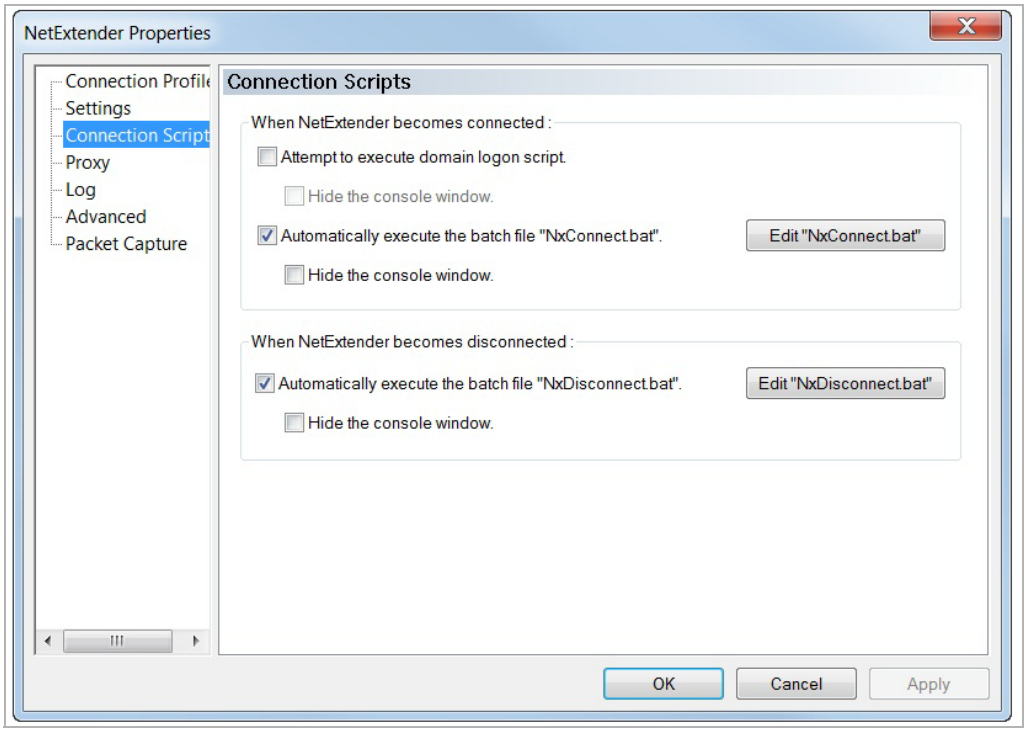
Step 14 Click **Apply**.

Configuring NetExtender Connection Scripts

Dell SonicWALL SSL VPN provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or Web sites. To configure NetExtender Connection Scripts, perform the following tasks.

Step 1 Right click on the icon in the task bar and click on **Properties...** The NetExtender Preferences window is displayed.

Step 2 Click on **Connection Scripts**.



Step 3 To enable the domain login script, select the **Attempt to execute domain logon script** check box. When enabled, NetExtender will attempt to contact the domain controller and execute the login script. Optionally, you may now also select to **Hide the console window**. If this check box is not selected, the DOS console window will remain open while the script runs.

Note Enabling this feature may cause connection delays while remote client's printers and drives are mapped. Make sure the domain controller and any machines in the logon script are accessible via NetExtender routes.

Step 4 To enable the script that runs when NetExtender connects, select the **Automatically execute the batch file "NxConnect.bat"** check box. Optionally, you may now also select to **Hide the console window**. If this check box is not selected, the DOS console window will remain open while the script runs.

Step 5 To enable the script that runs when NetExtender disconnects, select the **Automatically execute the batch file "NxDisconnect.bat"** check box.

Step 6 Click **Apply**.

Configuring Batch File Commands

NetExtender Connection Scripts can support any valid batch file commands. For more information on batch files, see the following Wikipedia entry: http://en.wikipedia.org/wiki/.bat. The following tasks provide an introduction to some commonly used batch file commands.

Step 1 To configure the script that runs when NetExtender connects, click the **Edit "NxConnect.bat"** button. The NxConnect.bat file is displayed.

Step 2 To configure the script that runs when NetExtender disconnects, click the **Edit "NxDisconnect.bat"** button. The NxConnect.bat file is displayed.

Step 3 By default, the **NxConnect.bat** file contains examples of commands that can be configured, but no actual commands. Too add commands, scroll to the bottom of the file.

Step 4 To map a network drive, enter a command in the following format:

net use *drive-letter**server**share password* **/user:***Domain**name*

For example to if the drive letter is **z**, the server name is **engineering**, the share is **docs**, the password is **1234**, the user's domain is **eng** and the username is **admin**, the command would be the following:

```
net use z\\engineering\docs 1234 /user:eng\admin
```

Step 5 To disconnect a network drive, enter a command in the following format:

net use *drive-letter*: **/delete**

For example, to disconnect network drive z, enter the following command:

```
net use z: /delete
```

Step 6 To map a network printer, enter a command in the following format:

net use LPT1 *ServerName**PrinterNa*me **/user:***Domain**name*

For example, if the server name is **engineering**, the printer name is **color-print1**, the domain name is **eng**, and the username is admin, the command would be the following:

```
net use LPT1 \\engineering\color-print1 /user:eng\admin
```

Step 7 To disconnect a network printer, enter a command in the following format:

```
net use LPT1 /delete
```

Step 8 To launch an application enter a command in the following format:

C:*Path-to-Application**Application.exe*

Step 9 For example, to launch Microsoft Outlook, enter the following command:

```
C:\Program Files\Microsoft Office\OFFICE11\outlook.exe
```

Step 10 To open a Web site in your default browser, enter a command in the following format:

start http://*www.website.com*

Step 11 To open a file on your computer, enter a command in the following format:

`C:\Path-to-file\myFile.doc`

Step 12 When you have finished editing the scripts, save the file and close it.

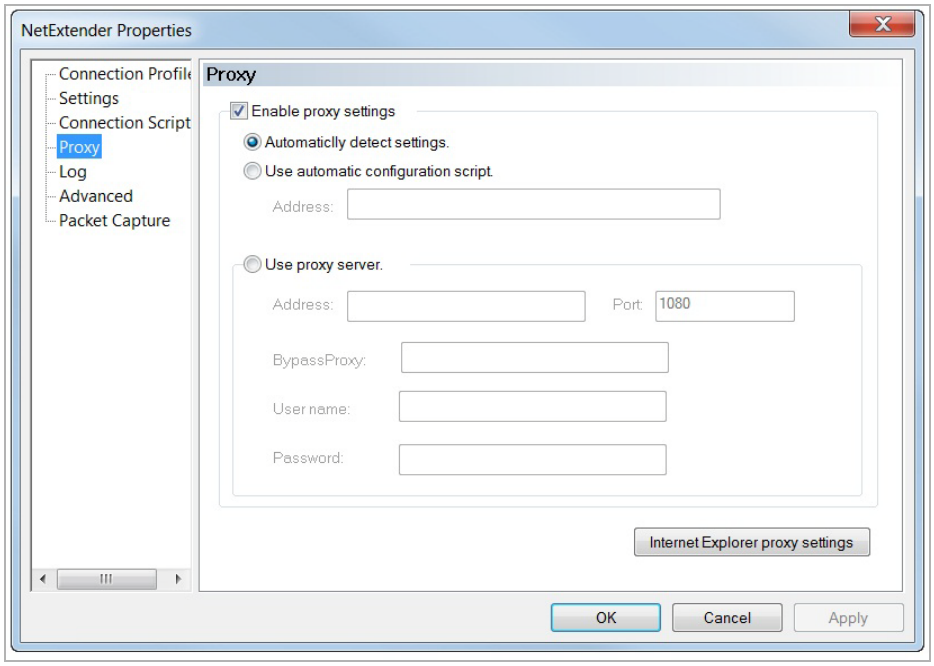
Configuring Proxy Settings

Dell SonicWALL SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the Web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings.

To manually configure NetExtender proxy settings, perform the following tasks.

Step 1 Right click on the icon in the task bar and click on **Preferences...** The NetExtender Preferences window is displayed.

Step 2 Click on **Proxy**.



Step 3 Select the **Enable proxy settings** check box.

Step 4 NetExtender provides three options for configuring proxy settings:

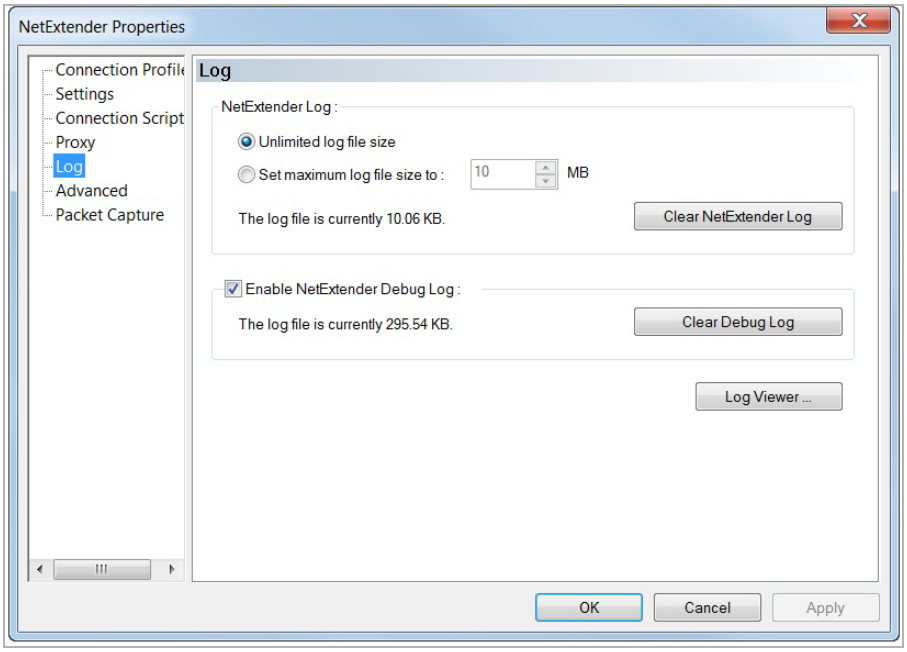
- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, select this option and enter the URL of the scrip in the Address field.
- **Use proxy server** - Select this option to enter the **Address** and **Port** of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses that bypass the proxy server. If required,

enter a **User name** and **Password** for the proxy server. If the proxy server requires a username and password, but you do not specify them in the **Properties** window, a NetExtender pop-up window will prompt you to enter them when you first connect.

Step 5 Click the **Internet Explorer proxy settings** button to open Internet Explorer's proxy settings.

Configuring NetExtender Log Properties

Within the NetExtender Properties dialog box, click on the **Log** heading in the menu on the left panel. The available options provide basic control over the NetExtender Log and Debug Log.



Step 1 To establish the size of the NetExtender Log, select either the **Unlimited log file size** radio button or the **Set maximum log file size to** radio button. If you choose to set a maximum size, use the adjoining arrows. To clear the NetExtender Log, select the **Clear NetExtender Log** button.

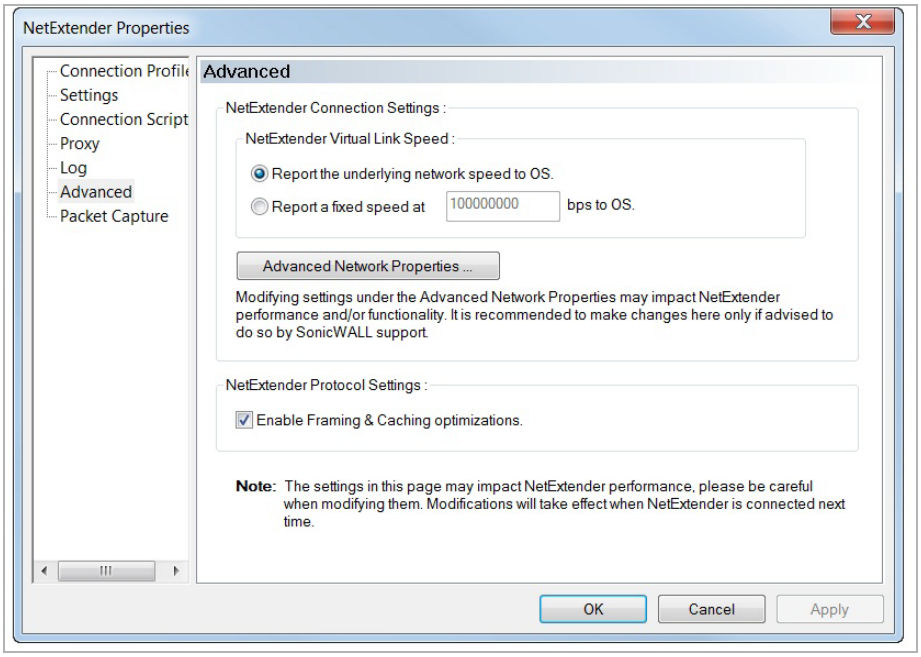
Step 2 To **Enable the NetExtender Debug Log**, select the corresponding check box. To clear the debug log, select the **Clear Debug Log** button.

Step 3 Click the **Log Viewer...** button to view the current NetExtender log.

Step 4 Click **Apply**.

Configuring NetExtender Advanced Properties

Within the NetExtender Properties dialog box, click on the **Advanced** heading in the menu on the left panel. The available options allow you to adjust advanced settings on NetExtender network properties and protocols.


NetExtender Properties
Connection Profile
Settings
Connection Script
Proxy
Log
Advanced
Packet Capture
Advanced
NetExtender Connection Settings :
NetExtender Virtual Link Speed :
Report the underlying network speed to OS.
Report a fixed speed at
100000000
bps to OS.
Advanced Network Properties ...
Modifying settings under the Advanced Network Properties may impact NetExtender performance and/or functionality. It is recommended to make changes here only if advised to do so by SonicWALL support.
NetExtender Protocol Settings :
Enable Framing & Caching optimizations.
Note: The settings in this page may impact NetExtender performance, please be careful when modifying them. Modifications will take effect when NetExtender is connected next time.
OK
Cancel
Apply

NetExtender allows users to customize the link speed that the NetExtender adapter reports to the operating system.

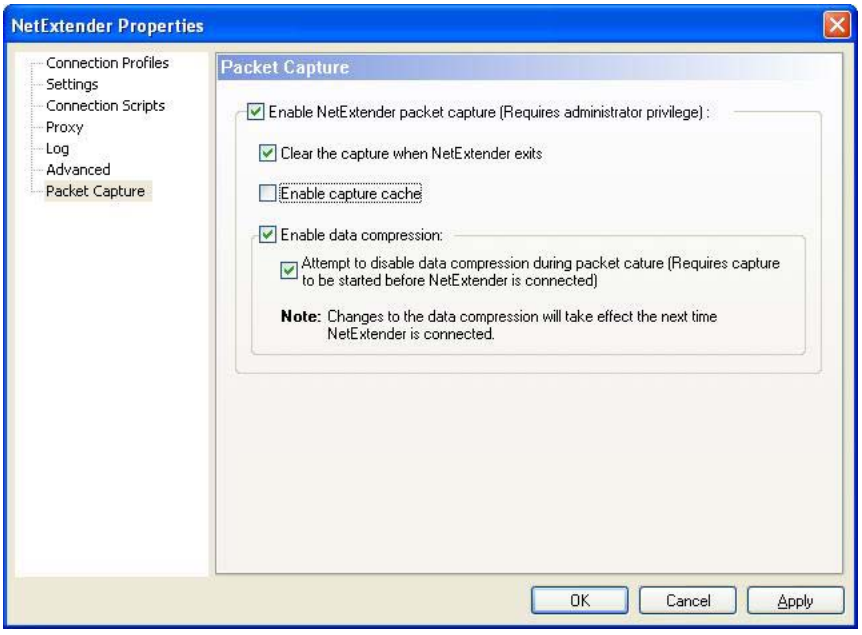
Step 1 To select a virtual link speed to report, select either the **Report the underlying network speed to OS** radio button, or select the **Report a fixed speed** radio button and designate a speed.

Note Users can click on the **Advanced Network Properties** button to make adjustments. However, modifying these settings may impact NetExtender performance and/or functionality. It is recommended to only make changes here if advised to do so by Dell SonicWALL support.

Step 2 Users may enable or disable Framing and Caching optimizations using the check box under NetExtender Protocol Settings. This option is only effective when connecting to a SSL VPN server running on 3.5 or later firmware.

Configuring NetExtender Packet Capture Properties

Within the NetExtender Properties dialog box, click on the **Packet Capture** heading in the menu on the left panel. The available options allow you to enable and disable packet capture and data compression on NetExtender.



Note You must have administrator privileges to change packet capture settings.

Step 1 To enable packet capture, check the **Enable NetExtender packet capture** check box.

Step 2 If packet capture is enabled, clear all captured packet data when NetExtender exits by checking the **Clear the capture when NetExtender exits** check box. To disable packet capture, uncheck this check box.

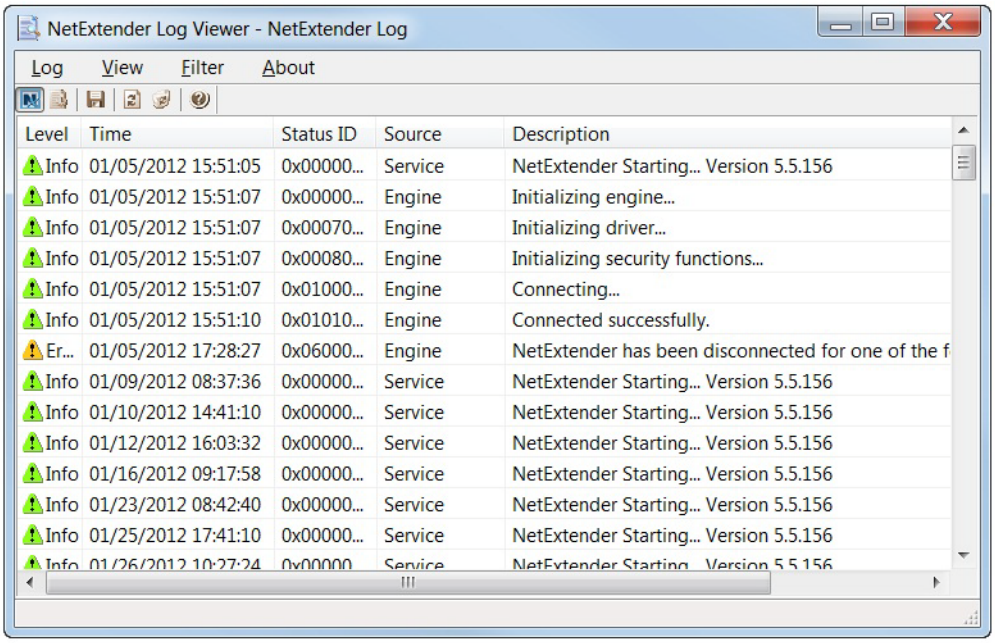
Step 3 If packet capture is enabled, clear all captured packet data when NetExtender exits by checking the **Clear the capture when NetExtender exits** check box. To retain packet data, uncheck this check box.

Step 4 To enable data compression of captured packets, check the **Enable data compression** check box. To disable data compression the next time NetExtender is connected, uncheck this box. If packet capture is enabled when NetExtender connects and you want to disable data compression immediately (instead of waiting until the next time NetExtender is connected), check the **Attempt to disable data compression during packet capture** check box.

Step 5 Click **Apply** to save your changes.

Viewing the NetExtender Log

The NetExtender log displays information on NetExtender session events. The log is a file named **NetExtender.dbg**. It is stored in the directory: C:\Program Files\SonicWALL\SSL VPN\NetExtender. To view the NetExtender log, right click on the NetExtender icon in the system tray, and click **View Log**, click on the Log icon on the main status page.

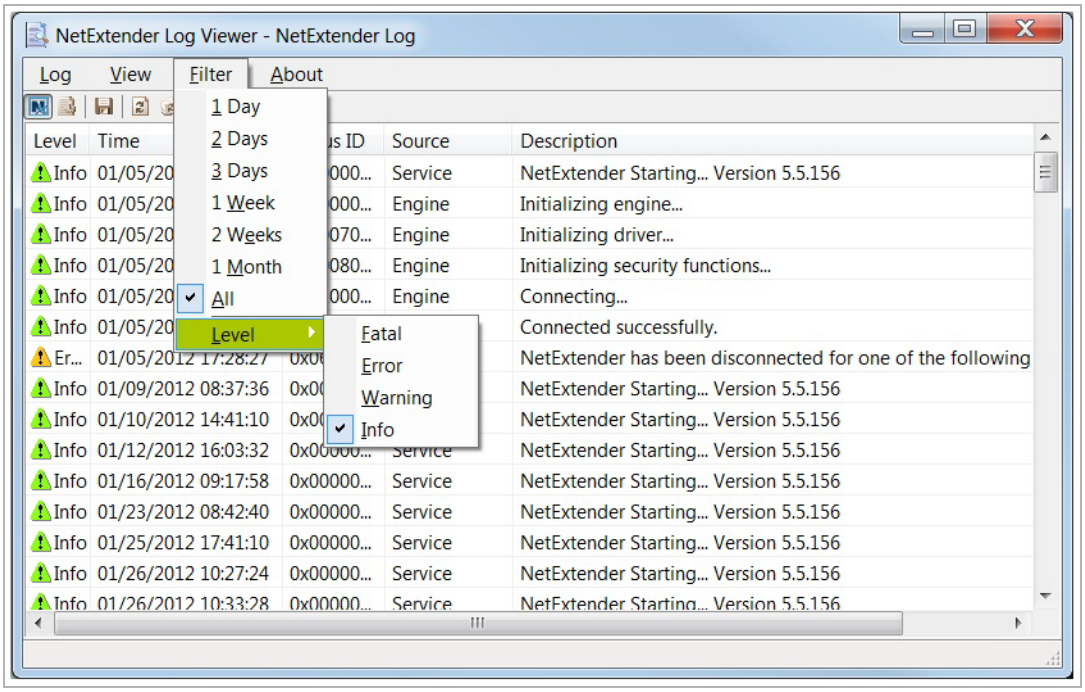

NetExtender Log Viewer - NetExtender Log
Log
View
Filter
About
Level Time Status ID Source Description
Info 01/05/2012 15:51:05 0x00000... Service NetExtender Starting... Version 5.5.156
Info 01/05/2012 15:51:07 0x00000... Engine Initializing engine...
Info 01/05/2012 15:51:07 0x00070... Engine Initializing driver...
Info 01/05/2012 15:51:07 0x00080... Engine Initializing security functions...
Info 01/05/2012 15:51:07 0x01000... Engine Connecting...
Info 01/05/2012 15:51:10 0x01010... Engine Connected successfully.
Er... 01/05/2012 17:28:27 0x06000... Engine NetExtender has been disconnected for one of the f
Info 01/09/2012 08:37:36 0x00000... Service NetExtender Starting... Version 5.5.156
Info 01/10/2012 14:41:10 0x00000... Service NetExtender Starting... Version 5.5.156
Info 01/12/2012 16:03:32 0x00000... Service NetExtender Starting... Version 5.5.156
Info 01/16/2012 09:17:58 0x00000... Service NetExtender Starting... Version 5.5.156
Info 01/23/2012 08:42:40 0x00000... Service NetExtender Starting... Version 5.5.156
Info 01/25/2012 17:41:10 0x00000... Service NetExtender Starting... Version 5.5.156

To view details of a log message, double-click on a log entry, or go to **View > Log Detail** to open the Log Detail pane.

To save the log, either click the **Export** icon or go to **Log > Export**.

To filter the log to display entries from a specific duration of time, go to the **Filter** menu and select the cutoff threshold.

To filter the log by type of entry, go to **Filter > Level** and select one of the level categories. The available options are **Fatal**, **Error**, **Warning**, and **Info**, in descending order of severity. The log displays all entries that match or exceed the severity level. For example, when selecting the **Error** level, the log displays all **Error** and **Fatal** entries, but not **Warning** or **Info** entries.



To view the Debug Log, either click the **Debug Log** icon or go to **Log > Debug Log**.

Note It may take several minutes for the Debug Log to load. During this time, the Log window will not be accessible, although you can open a new Log window while the Debug Log is loading.

To clear the log, click on **Log > Clear Log**.

Disconnecting NetExtender

To disconnect NetExtender, perform the following steps:

Step 1 Right click on the NetExtender icon in the system tray to display the NetExtender icon menu and click **Disconnect**.

Step 2 Wait several seconds. The NetExtender session disconnects.

You can also disconnect by double clicking on the NetExtender icon to open the **NetExtender** window and then clicking the **Disconnect** button.

When NetExtender becomes disconnected, the NetExtender window displays and gives you the option to either **Reconnect** or **Close** NetExtender.

Upgrading NetExtender

NetExtender automatically notifies users when an updated version of NetExtender is available. Users are prompted to click **OK** and NetExtender downloads and installs the update from the Dell SonicWALL SRA security appliance.

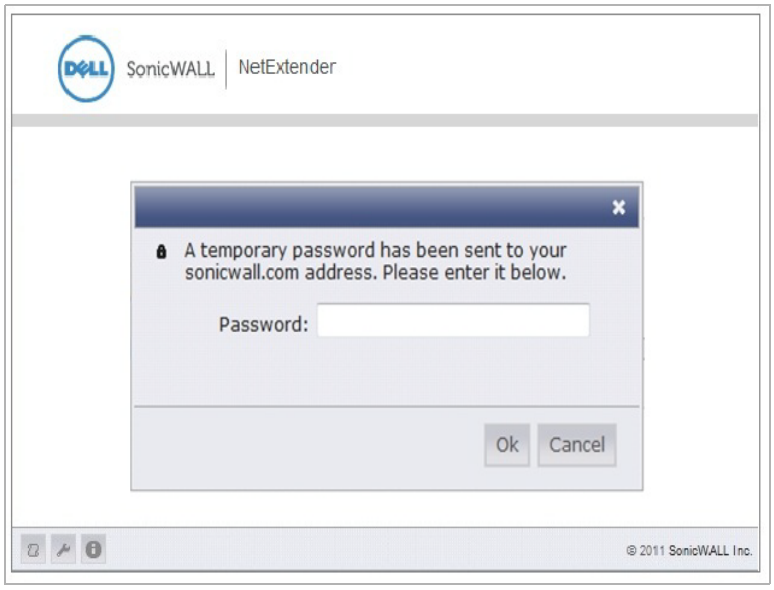
When using releases prior to 2.5, users should periodically launch NetExtender from the Dell SonicWALL Virtual Office to ensure they have the latest version. Prior to release 2.5, the standalone NetExtender does not check for updates when it is launched directly from a user's computer.

Changing Passwords

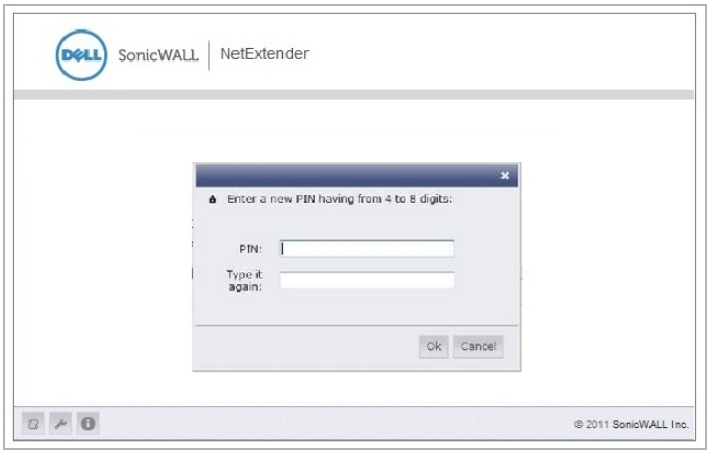
Before connecting to the new version of NetExtender, users may be required to reset their password by suppling their old password, along with providing and re-verifying a new one.

Authentication Methods

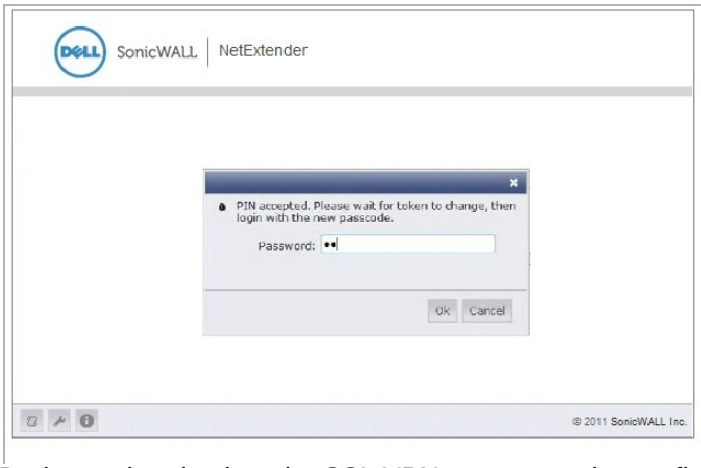
NetExtender supports various two factor authentication methods, including one-time password, RSA, and Vasco. If an administrator has configured one-time passwords to be required to connect through NetExtender, you will be asked to provide this information before connecting.



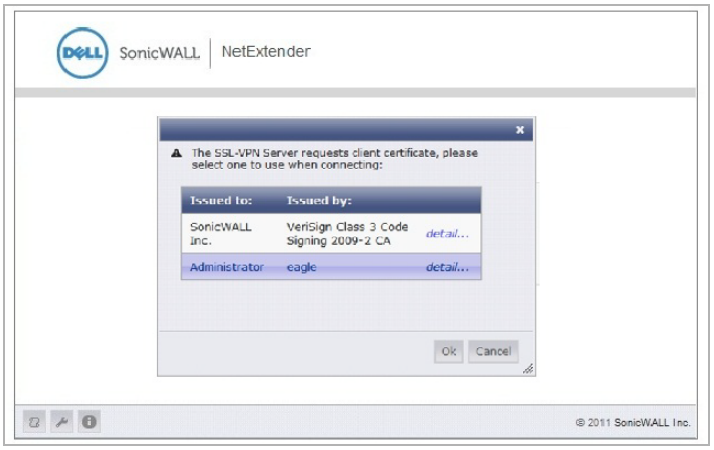
If an administrator has configured RSA pin-mode authentication to be required to connect through NetExtender, users will be asked whether they want to create their own pin, or receive one that is system-generated.



Once the pin has been accepted, you must wait for the token to change before logging in to NetExtender with the new passcode.



During authentication, the SSL VPN server may be configured by the administrator to request a client certificate. In this case, users must select a client certificate to use when connecting.



Uninstalling NetExtender

The NetExtender utility is automatically installed on your computer. To remove NetExtender, click on **Start > All Programs**, click on **Dell SonicWALL NetExtender**, and then click on **Uninstall**.

You can also configure NetExtender to automatically uninstall when your session is disconnected. To do so, perform the following steps:

Step 1 Right click on the NetExtender icon in the system tray and click on **Properties**... The **NetExtender Properties** window is displayed.

Step 2 Click on the **Settings** tab.

Step 3 Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

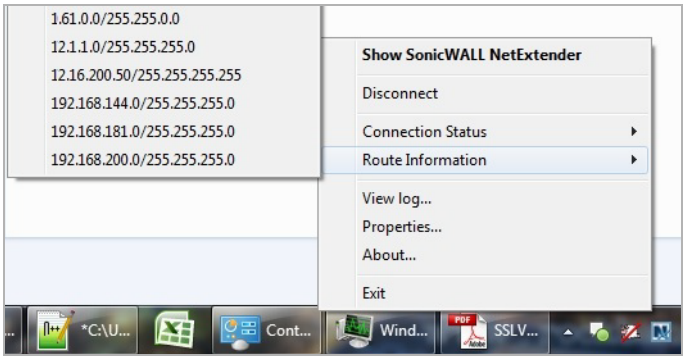
Step 4 Click **Apply**.

Verifying NetExtender Operation from the System Tray

To view options in the NetExtender system tray, right click on the NetExtender icon in the system tray. The following are some tasks you can perform with the system tray.

Displaying Route Information

To display the routes that NetExtender has installed on your system, click the **Route Information** option in the system tray menu. The system tray menu displays the default route and the associated subnet mask.



Displaying Connection Information

You can display connection information by mousing over the NetExtender icon in the system tray.

Using the NetExtender Command Line Interface

Note The NetExtender command line interface is only available on Windows platforms.

To launch the NetExtender CLI, perform the following tasks:

Step 1 Launch the Windows Command Prompt by going to the **Start** menu, select **Run**, enter **cmd**, and click **OK**.

Step 2 Change directory to where NetExtender is installed. To do this, you first must move up to the root drive by entering the **cd ..** command. Repeat this command until you are at the root drive. Then enter **cd Program Files\SonicWALL\SSL-VPN\NetExtender**.

Note The specific command directory may be different on your computer. Use Windows Explorer to find the directory path where NetExtender is located.

The following table describes the commands available in the NetExtender CLI and their options.

Table 1 NetExtender CLI Commands

Command	Option	Description
NECLI addprofile		Creates a NetExtender profile
	-s *server*	The IP address or hostname of the SSL VPN server.
	-u *user-name*	The username for the account.
	-p *password*	The password for the account.
	-d *domain-name*	The domain to connect to.
NECLI connect		Initiates a NetExtender session.
	-s *server*	The IP address or hostname of the SSL VPN server.
	-u *user-name*	The username for the account.
	-p *password*	The password for the account.
	-d *domain-name*	The domain to connect to.
	- **clientcertificatethumb** *thumb*	The SSL Client Certificate thumbprint value.
	- **clientcertificatename** *name*	The SSL Client Certificate name.
NECLI deleteprofile		Deletes a saved NetExtender profile.
	-s *server*	The IP address or hostname of the SSL VPN server.
	-u *user-name*	The username for the account.
	-d *domain-name*	The domain to connect to.
NECLI disconnect		Disconnects
	timeout	(Optional) Timeout duration, after which the session is disconnected.

Table 1 NetExtender CLI Commands

Command	Option	Description
NECLI displayprofile		Displays all NetExtender profiles.
	-s *server*	(Optional) Displays only the profiles that are saved for the specified server.
	-u *user-name*	(Optional) Displays only the profiles that are saved for the specified user name.
	-d *domain-name*	(Optional) Displays only the profiles that are saved for the specified domain name.
NECLI queryproxy		Checks the connect to the proxy server.
NECLI reconnect		Attempts to reconnect to the server.
NECLI showstatus		Displays the status of the current NetExtender session.
NECLI setproxy		Configures proxy settings for NetExtender.
	-t [**0** |**1** | **2** | **3**]	There are three options for setting proxy settings: 0 - Disable proxy. **1** - Automatically detects proxy settings. The proxy server must support Web Proxy Auto Discovery Protocol (WPAD). **2** - Uses a proxy configuration script. **3** - Manually configure the proxy server.
	-s proxy address	The address of the proxy script or proxy server.
	-o port	The port number.
	-u user name	The user name for the proxy server.
	-p password	The password name for the proxy server.
	-b bypass-proxy	Bypasses the previously configured proxy settings.
	-save	Saves the proxy settings.
NECLI viewlog		Displays the NetExtender log.

Installing NetExtender on MacOS

Dell SonicWALL SSL VPN supports NetExtender on MacOS. To use NetExtender on your MacOS system, your system must meet the following prerequisites:

- Mac OS 10.6 and higher
- Java 1.5 and higher
- Both PowerPC and Intel Macs are supported.

To install NetExtender on your MacOS system, perform the following tasks:

Step 1 Log in to the Dell SonicWALL Virtual Office.

Step 2 Click the **NetExtender** button.

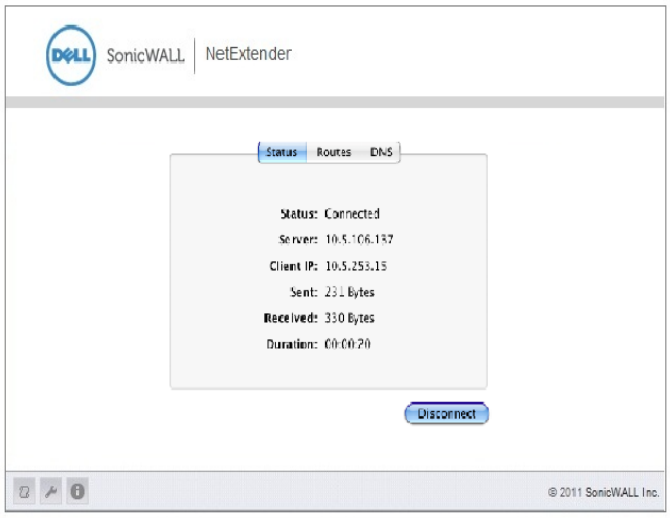
Step 3 The Virtual Office displays the status of NetExtender installation. A pop-up window may appear, prompting you to accept a certificate. Click **Trust**.

SonicWALL – Virtual Office
NetExtender for Mac OS X
In the future, you can launch NetExtender from your Applications folder without returning to this web page.
Close this window
10.5.106.137
Do you want to accept this certificate from the web site "10.5.106.137" for the purpose of exchanging encrypted information?
Publisher authenticity can not be verified.
Show Certificate
Don't Trust
Trust

Step 4 A second pop-up window may appear, prompting you to accept a certificate. Click **Trust**.

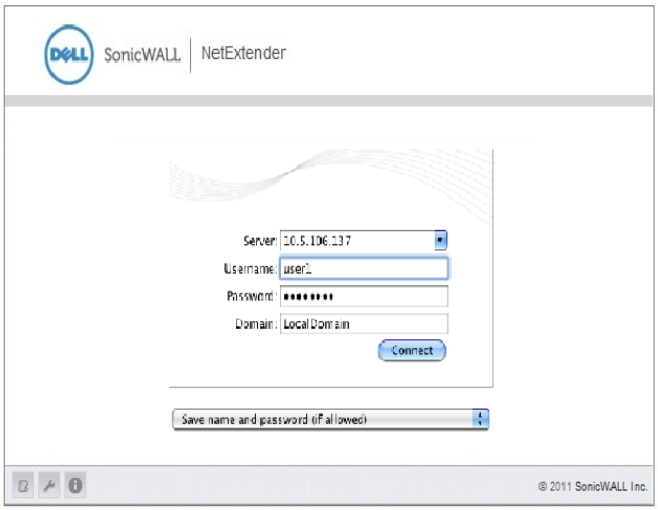
An applet from "10.5.106.137" is requesting access to your computer.
The digital signature from "SonicWALL Inc." has been verified.
Allow all applets from "10.5.106.137" with this signature
Show Details...
Deny
Allow

Step 5 When NetExtender is successfully installed and connected, the NetExtender status window displays.



Using NetExtender on MacOS

Step 1 To launch NetExtender, go the **Applications** folder in the **Finder** and double click on **NetExtender.app**.



Step 2 The first time you connect, you must enter the Dell SonicWALL SSL VPN server name in the **SSL VPN Server** field.

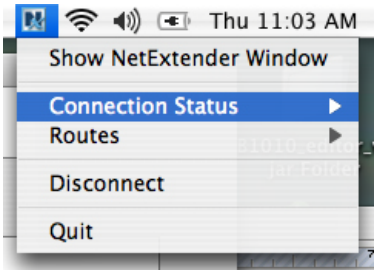
Step 3 Enter your username and password.

Step 4 The first time you connect, you must enter the **domain** name. The domain name is case-sensitive.

Step 5 Click **Connect**.

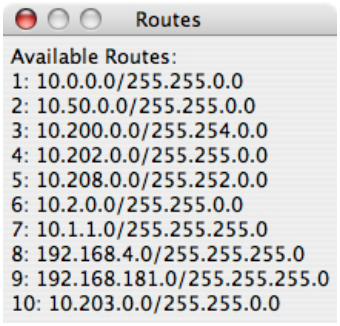
Step 6 You can instruct NetExtender remember your profile server name in the future. In the **Save profile** drop-down menu you can select **Save name and password (if allowed)**, **Save username only (if allowed)**, or **Do not save profile**.

Step 7 When NetExtender is connected, the NetExtender icon is displayed in the status bar at the top right of your display. Click on the icon to display NetExtender options.

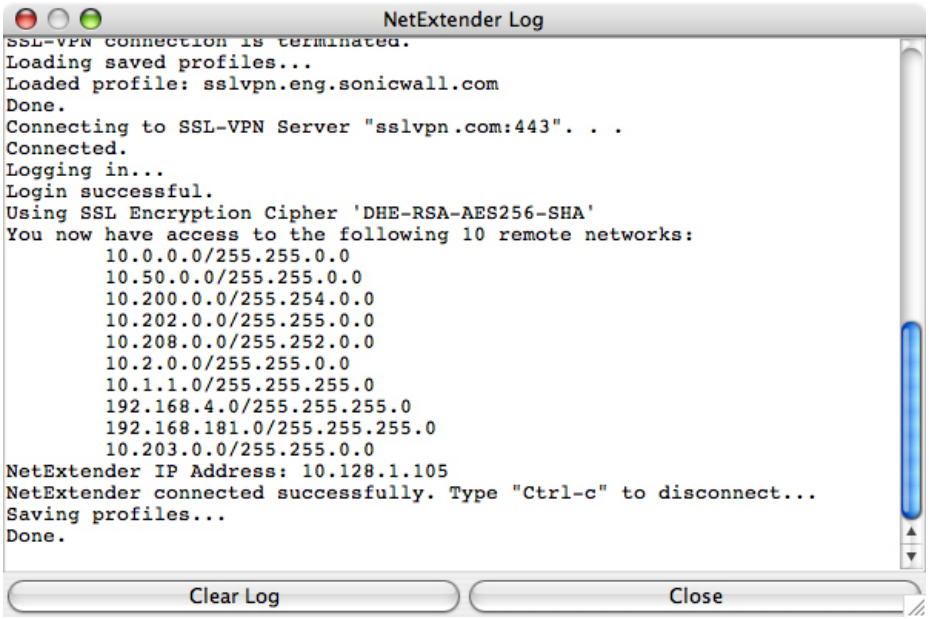


Step 8 To display a summary of your NetExtender session, click **Connection Status.**

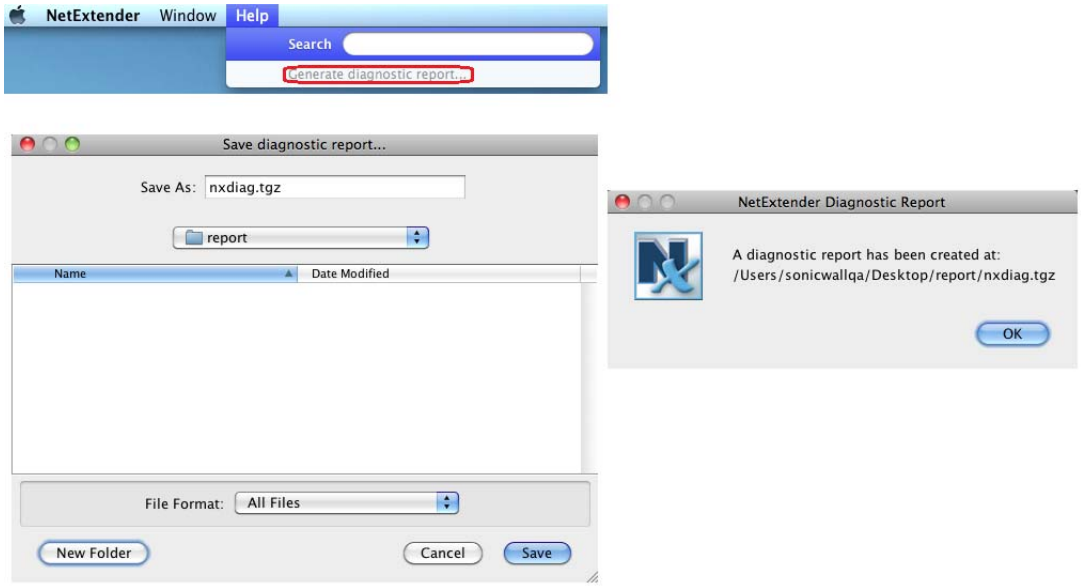
Step 9 To view the routes that NetExtender has installed, select the **Routes** tab in the main NetExtender window.



Step 10 To view the NetExtender Log, go to **Window > Log**.



Step 11 To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.



Step 12 Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

Installing NetExtender on Linux

Dell SonicWALL SSL VPN supports NetExtender on Linux. To use NetExtender on your Linux system, your system must meet the following prerequisites:

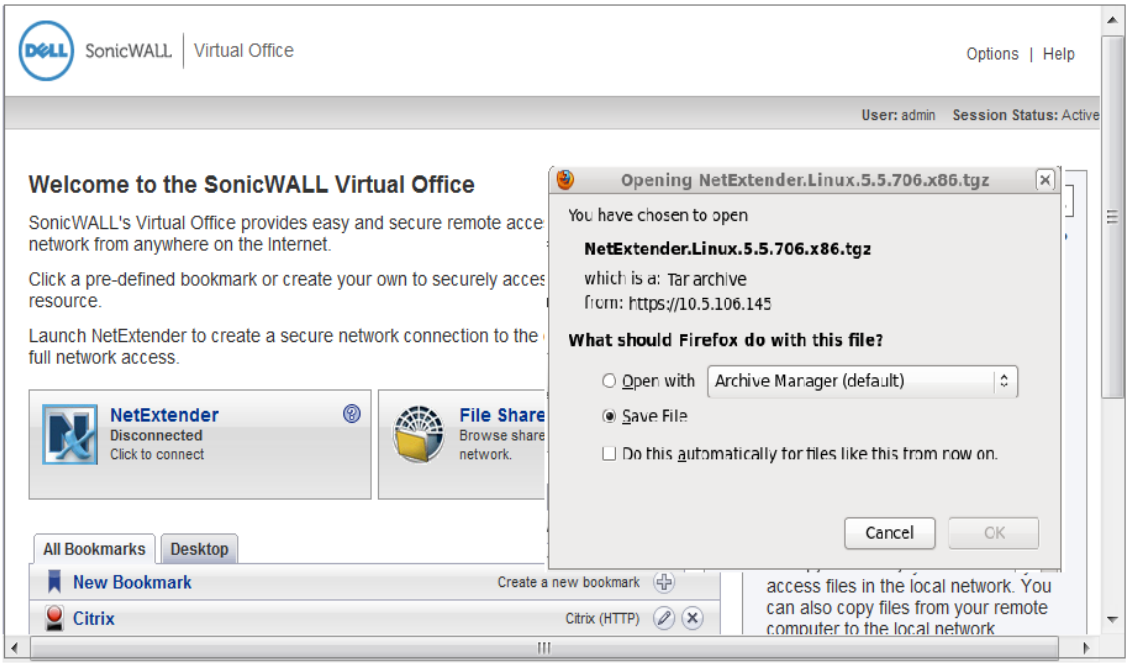
- i386-compatible distribution of Linux
- Linux Fedora Core 15 or higher, Ubuntu 11.10 or higher, or OpenSUSE 10.3 or higher
- Java 1.5 and higher is required for using the NetExtender GUI.

Note Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Java 1.5, you can use the command-line interface version of NetExtender.

To install NetExtender on your Linux system, perform the following tasks:

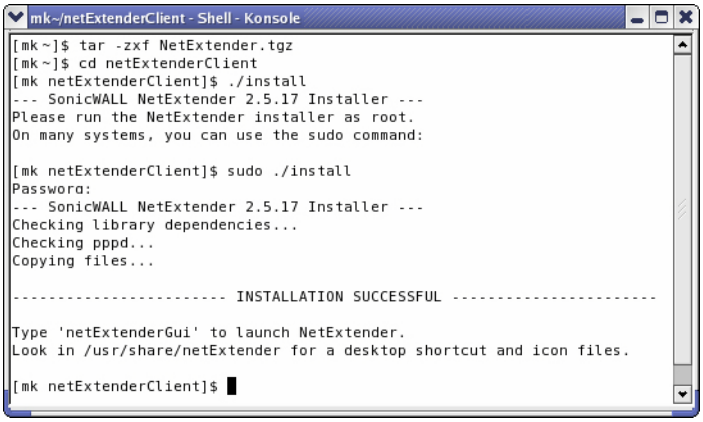
Step 1 Log in to the Dell SonicWALL Virtual Office.

Step 2 Click the **NetExtender** button. A pop-up window indicates that you have chosen to open a **.tgz** file. Click **OK** to save it to your default download directory.



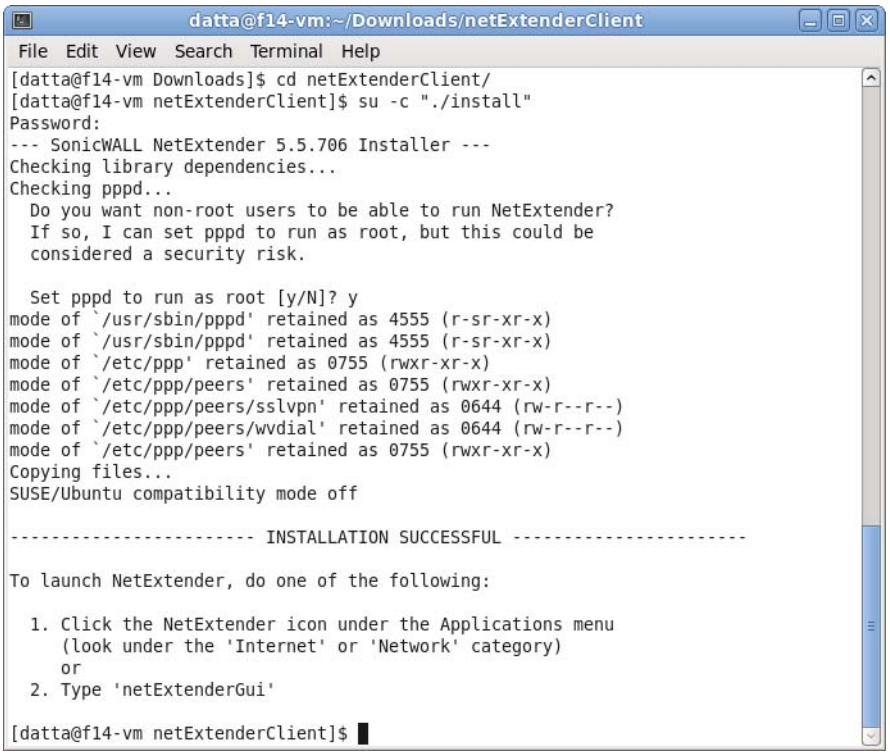
Note You must be logged in as root to install NetExtender, although many Linux systems will allow the **sudo ./install** command to be used if you are not logged in as root.

Step 3 To install NetExtender from the CLI, navigate to the directory where you saved the **.tgz** file and enter the **tar -zxf NetExtender.tgz** command.


mk~/netExtenderClient - Shell - Konsole
[mk~]$ tar -zxf NetExtender.tgz
[mk~]$ cd netExtenderClient
[mk netExtenderClient]$ ./install
--- SonicWALL NetExtender 2.5.17 Installer ---
Please run the NetExtender installer as root.
On many systems, you can use the sudo command:
[mk netExtenderClient]$ sudo ./install
Password:
--- SonicWALL NetExtender 2.5.17 Installer ---
Checking library dependencies...
Checking pppd...
Copying files...
---------- INSTALLATION SUCCESSFUL ----------
Type 'netExtenderGui' to launch NetExtender.
Look in /usr/share/netExtender for a desktop shortcut and icon files.
[mk netExtenderClient]$

Step 4 Enter the **cd netExtenderClient/** command.

Step 5 Enter **su -C** " **./install"** to install NetExtender.


datta@f14-vm:~/Downloads/netExtenderClient
File Edit View Search Terminal Help
[datta@f14-vm Downloads]$ cd netExtenderClient/
[datta@f14-vm netExtenderClient]$ su -c "./install"
Password:
--- SonicWALL NetExtender 5.5.706 Installer ---
Checking library dependencies...
Checking pppd...
Do you want non-root users to be able to run NetExtender?
If so, I can set pppd to run as root, but this could be
considered a security risk.
Set pppd to run as root [y/N]? y
mode of `/usr/sbin/pppd' retained as 4555 (r-sr-xr-x)
mode of `/usr/sbin/pppd' retained as 4555 (r-sr-xr-x)
mode of `/etc/ppp' retained as 0755 (rwxr-xr-x)
mode of `/etc/ppp/peers' retained as 0755 (rwxr-xr-x)
mode of `/etc/ppp/peers/sslvpn' retained as 0644 (rw-r--r--)
mode of `/etc/ppp/peers/wvdial' retained as 0644 (rw-r--r--)
mode of `/etc/ppp/peers' retained as 0755 (rwxr-xr-x)
Copying files...
SUSE/Ubuntu compatibility mode off
---------- INSTALLATION SUCCESSFUL ----------
To launch NetExtender, do one of the following:
1. Click the NetExtender icon under the Applications menu
(look under the 'Internet' or 'Network' category)
or
2. Type 'netExtenderGui'
[datta@f14-vm netExtenderClient]$

Step 6 Enter your system password.

Step 7 The installer will ask if you want non-root users to be able to run NetExtender. Enter either **y** for yes or **n** for no.

Note To allow non-root users to run NetExtender, the installer will set PPPD to run as root. This may be considered a security risk.

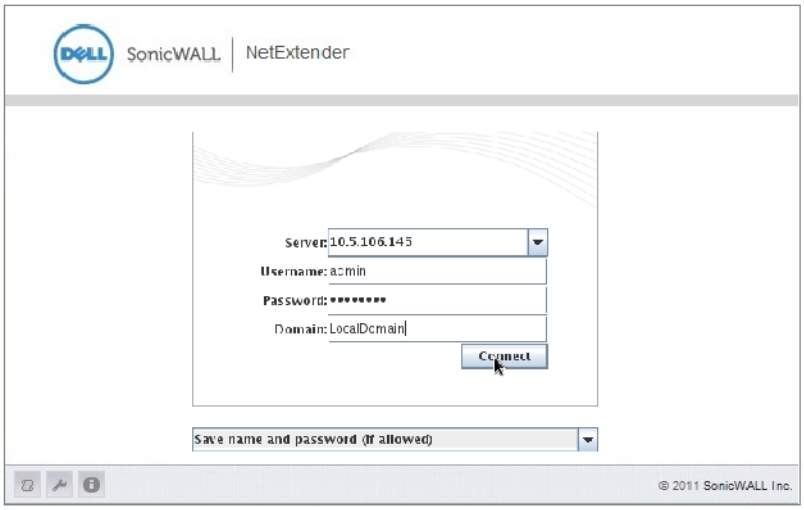
Using NetExtender on Linux

To use NetExtender on a Linux computer, perform the following tasks:

Step 1 After NetExtender is installed, there are two methods to launch it:

- Click the NetExtender icon in the Applications menu, under either the **Internet** or **Network** category.
- Enter the **netExtenderGui** command.

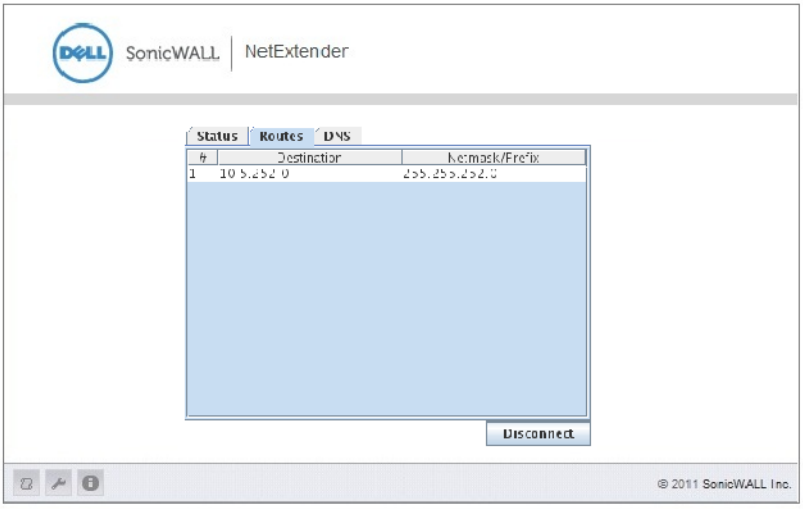
Step 2 The first time you connect, you must enter the Dell SonicWALL SSL VPN server name in the **SSL VPN Server** field. NetExtender will remember the server name in the future.



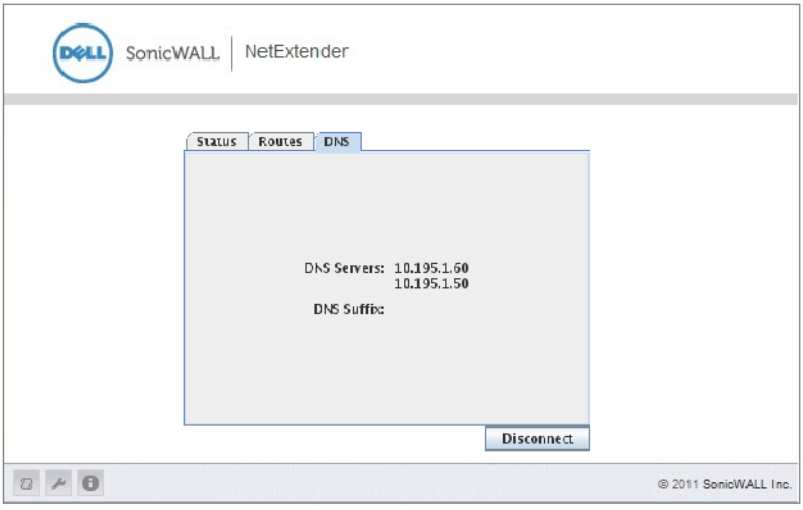
Step 3 Enter your username and password.

Step 4 The first time you connect, you must enter the **domain** name. The domain name is case-sensitive. NetExtender will remember the domain name in the future.

Step 5 To view the NetExtender routes, select the **Routes** tab in the main NetExtender window.



Step 6 To view the NetExtender DNS server information, select the **DNS** tab in the main NetExtender window.



Step 7 To configure NetExtender Preferences, select **NetExtender > Preferences**.

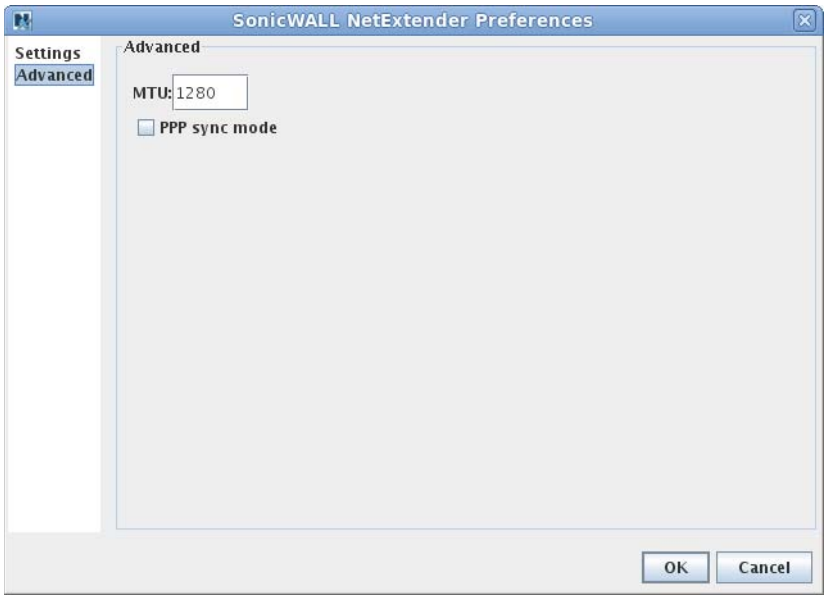
Step 8 The following NetExtender settings can be configured:

- Automatically reconnect when the connection is terminated
- Uninstall NetExtender automatically when exiting the application
- DNS server options:
  - Try remote DNS servers first, then try local DNS servers
  - Only use remote DNS servers
  - Only use local DNS servers

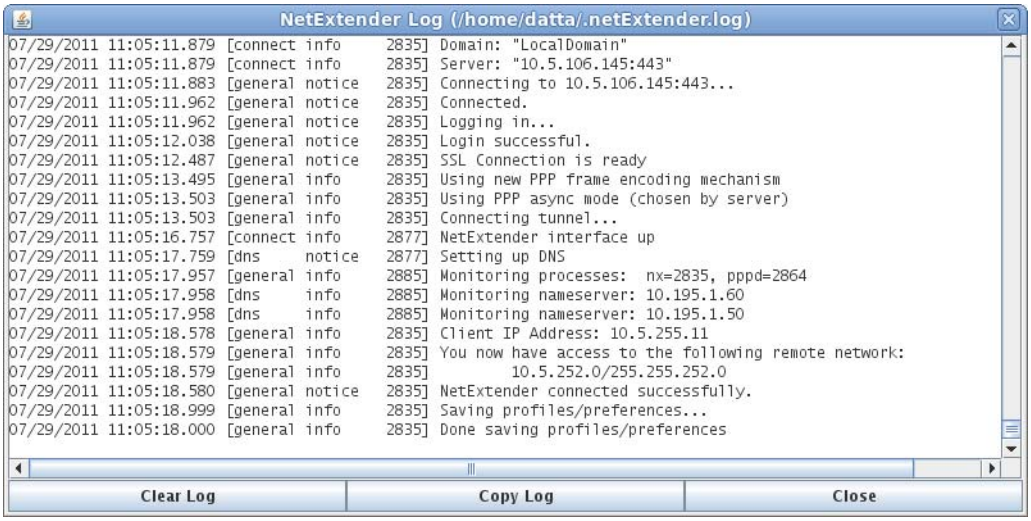
Step 9 The Advanced tab of the NetExtender Preferences window provides two additional options:

- MTU - Sets the Maximum Transmission Unit (MTU) size, which is the largest packet size that a router can forward without needing to fragment the packet.

- PPP Sync Mode - Specifies synchronous PPP. By default, this option is disabled and asynchronous PPP is used.



Step 10 To view the NetExtender Log, go to **NetExtender > Log**.


NetExtender Log (/home/datta/.netExtender.log)
07/29/2011 11:05:11.879 [connect info 2835] Domain: "LocalDomain"
07/29/2011 11:05:11.879 [connect info 2835] Server: "10.5.106.145:443"
07/29/2011 11:05:11.883 [general notice 2835] Connecting to 10.5.106.145:443...
07/29/2011 11:05:11.962 [general notice 2835] Connected.
07/29/2011 11:05:11.962 [general notice 2835] Logging in...
07/29/2011 11:05:12.038 [general notice 2835] Login successful.
07/29/2011 11:05:12.487 [general notice 2835] SSL Connection is ready
07/29/2011 11:05:13.495 [general info 2835] Using new PPP frame encoding mechanism
07/29/2011 11:05:13.503 [general info 2835] Using PPP async mode (chosen by server)
07/29/2011 11:05:13.503 [general info 2835] Connecting tunnel...
07/29/2011 11:05:16.757 [connect info 2877] NetExtender interface up
07/29/2011 11:05:17.759 [dns notice 2877] Setting up DNS
07/29/2011 11:05:17.957 [general info 2885] Monitoring processes: nx=2835, pppd=2864
07/29/2011 11:05:17.958 [dns info 2885] Monitoring nameserver: 10.195.1.60
07/29/2011 11:05:17.958 [dns info 2885] Monitoring nameserver: 10.195.1.50
07/29/2011 11:05:18.578 [general info 2835] Client IP Address: 10.5.255.11
07/29/2011 11:05:18.579 [general info 2835] You now have access to the following remote network:
07/29/2011 11:05:18.579 [general info 2835] 10.5.252.0/255.255.252.0
07/29/2011 11:05:18.580 [general notice 2835] NetExtender connected successfully.
07/29/2011 11:05:18.999 [general info 2835] Saving profiles/preferences...
07/29/2011 11:05:18.000 [general info 2835] Done saving profiles/preferences
Clear Log
Copy Log
Close

Step 11 To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.

Step 12 Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

Installing and Using NetExtender for Windows Mobile

Dell SonicWALL SSL VPN now supports NetExtender for the Windows Mobile platform. NetExtender for Windows Mobile provides the following features:

- One-time passwords
- Two-factor authentication
- HTTP proxy

- Connection profiles

NetExtender supports the following Windows Mobile platforms:

- Windows Mobile 5 PocketPC version
- Windows Mobile 6 Professional/Classic version

Note Windows Mobile 5 Smart Phone version and Windows Mobile 6 Standard version are not currently supported.

To use NetExtender on your Windows Mobile device, perform the following tasks:

Step 1 Navigate to the URL or IP address for your SSL VPN Virtual Office using the browser in your Windows Mobile device.

Step 2 Log in with your username and password.

Step 3 Click on the **NetExtender** icon.

Step 4 Follow the on-screen instructions to install NetExtender. When NetExtender is installed, you may be prompted to restart your device. Click **Yes**.

Step 5 From your Windows Mobile device, launch NetExtender. The NetExtender login screen displays.

Step 6 Enter the IP address or domain name for your SSL VPN server in the **Server** field. The IP address of the last SSL VPN server you connected to is displayed by default. To display a list of recent SSL VPN servers you have connected to, click on the arrow.

Step 7 Enter your username and password.

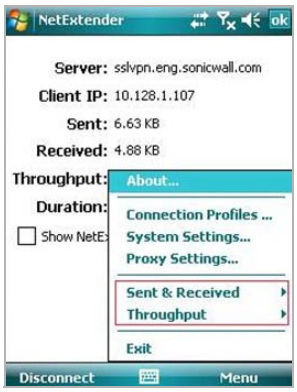
Step 8 The last domain you connected to is displayed in the **Domain** field.

Step 9 The drop-down menu at the bottom of the window provides three options for remembering your username and password:

- Save user name & password if server allows
- Save user name only if server allows
- Always ask for user name & password

Step 10 Click **Connect**. When NetExtender successfully connects, the **NetExtender Status** window displays. Select the **Show NetExtender Routes** check box to see routes.

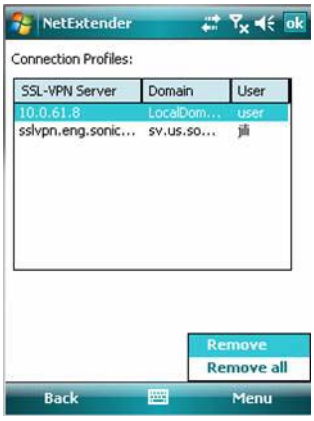
Step 11 Click on the **Menu** button to see the NetExtender properties menu.



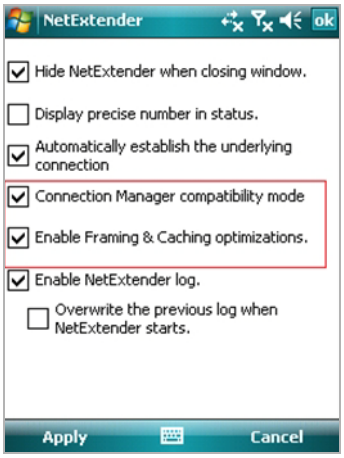
Step 12 Select the **Sent & Received** menu tab to adjust the metric used for sent and received statistics on the status window. Select the **Throughput** menu tab to adjust the throughput measurement displayed on the status window.

Step 13 To configure NetExtender options, click the **Menu** button. The following options are displayed:

- **Connection Profiles** - Displays all of the NetExtender connections that you have used on this device. To remove a Connection Profile, highlight the profile, click the **Menu** button, and click **Remove**.



- **System Settings** - Provides several configuration options.



- **Hide NetExtender when closing window** - Hides NetExtender when you click the **ok** button.
- **Display precise number in status** - Displays the exact numbers of sent and receive data.
- **Automatically establish the underlying connection** - Uses the Windows Mobile Connection Manager to establish the device's connection to the mobile network. The Connection Manage is designed to determine the optimum network type (such as 3g or wi-fi). If this option is disabled, the user manages the connection manually.
- **Connection Manager compatibility mode** - This mode is enabled by default to make NetExtender Mobile work with applications calling the Microsoft Connection Manager API. In limited cases, server applications may not work properly through NetExtender Mobile, so users can use this selection to disable the compatibility mode

Note If a user disables the Connection Manager compatibility mode, a confirmation message will prompt the user that this may cause some applications using the Connection Manager API to not work properly.

- **Enable Framing & Caching optimizations** - This setting increases the performance of NetExtender Mobile when it is under a heavy load, such as when downloading big files over NetExtender.
- **Enable NetExtender log** - Records log entries for NetExtender events.
- **Overwrite the previous log when NetExtender starts** - Maintains a single NetExtender log file that is overwritten with each new NetExtender session. Disabling this option will create a separate log file for each NetExtender session.

- **Proxy Settings** - Provides the ability to manually specify a proxy server.

Passwords in NetExtender Mobile

NetExtender Mobile supports the ability for users to change passwords. Also, if configured by an administrator, users can be alerted that the their password is scheduled to expire soon. If a user must change their password, a screen prompt will ask for the user's old password, along with a new password and re-verification of the new password.

Another screen prompt will be presented to the user, if their password is scheduled to expire within a configured number of days by the administrator. Click **Yes** to enter updated password information.

The process for updating password information is the same as above.

Installing NetExtender on Android Smartphones

Dell SonicWALL SSL VPN supports NetExtender on smartphones running the Android operating system. The NetExtender Android client supports the following features:

- One-time passwords
- Two-factor authentication
- HTTP/HTTPS proxy
- Connection profiles

The NetExtender Android installer is available on MySonicWALL in the standard **apk** package format. The installer is also available from Android Market as the NetExtender Technology Preview.

The following features are not supported or not applicable on NetExtender Android in Dell SonicWALL SSL VPN:

- Automatic connection of NetExtender before Windows login
- Automatic proxy support and Internet Explorer proxy synchronization
- Connection scripts
- IPv6 support
- Client certificate support
- Exit client after disconnect

To install NetExtender on an Android smartphone using the **apk** package from MySonicWALL, perform the following tasks:

Step 1 On a computer, log in to http://mySonicWALL.com.

Step 2 Click on **Downloads**.

Step 3 In the **Software Type** drop-down menu, select one of the following:

- SRA 4200 Firmware
- SRA 1200 Firmware
- SRA VM

Step 4 Click on the **NetExtender (Android)** link.

Step 5 Save the **.apk** file onto your computer.

Step 6 Using the USB cable, connect your computer to the Android smartphone.

Step 7 On the Android smartphone, pull down the notifications.

Step 8 Tap **USB connected** to connect to the computer. The next screen shows the connection.

1:35 PM
USB Mass Storage
USB connected
You have connected your phone to your computer via USB. Select the button below if you want to copy files between your computer and your Android's SD card.
Turn on USB storage

Step 9 Tap **Turn on USB storage** to prepare for copying the **apk** installer to the Android smartphone.

1:36 PM
USB Mass Storage
USB storage in use
Before turning off USB storage, make sure you have unmounted ("ejected") your Android's SD card from your computer.
Turn off USB storage

Step 10 On the computer, copy the **apk** file to the Android SD card.

Step 11 Unmount the Android SD card from your computer. On Windows, it will show up under "My Computer" as a new drive. On Mac, a new drive will show up on the desktop.

Step 12 After unmounting the Android SD card from your computer, tap **Turn off USB storage**.

Step 13 On your Android smartphone, launch a file browser application.

Step 14 Using the file browser, locate the **apk** file and run it to install NetExtender Android. After installation, the NetExtender icon appears on the applications page of the smartphone.

Using NetExtender on Android Smartphones

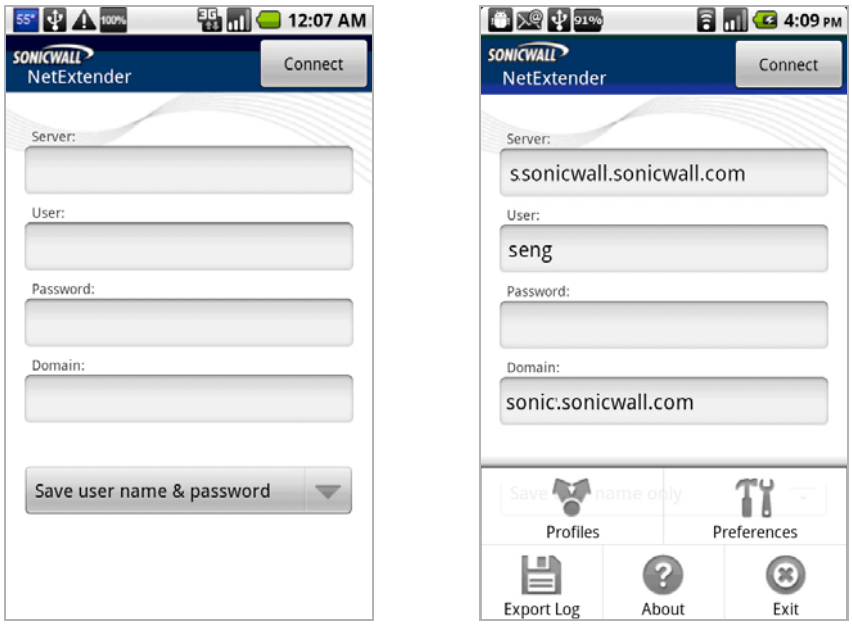
Instructions for using NetExtender on your Android smartphone are available in the following sections:

- “Connecting to NetExtender” on page 65
- “Exiting or Disconnecting from NetExtender” on page 69
- “Checking Status, Routes, and DNS Settings” on page 70
- “Configuring Profiles, Preferences, and Proxy Servers” on page 72
- “Changing Your Password” on page 75

Connecting to NetExtender

To launch NetExtender on your Android smartphone and connect to the network through the Dell SonicWALL SRA appliance, perform the following steps:

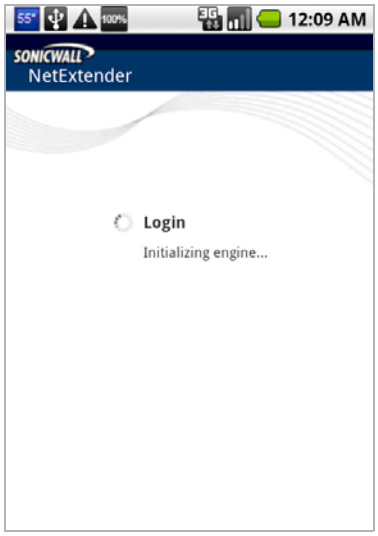
Step 1 On your Android smartphone, start NetExtender by tapping the application icon. The NetExtender connection options screen displays. Enter the information into the **Server**, **User**, **Password**, and **Domain** fields.



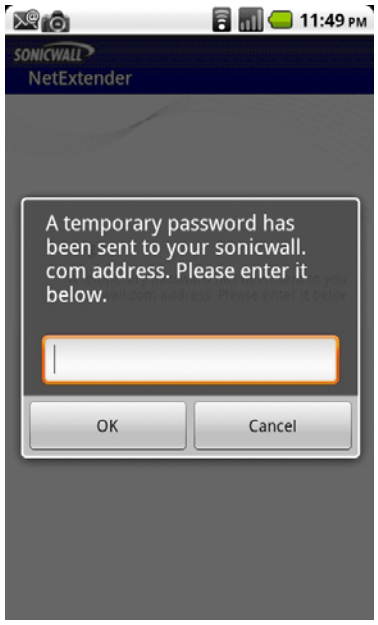
Step 2 Tap **Connect** to accept the default option (**Save user name & password**) or select a **Save...** or **Always ask...** option from the drop-down list. The available profile options depend on how NetExtender is configured on the Dell SonicWALL appliance.

Step 3 The smartphone displays the **Login - Initializing engine** screen.

After a successful connection, the entered values are saved as a profile that you can select when starting NetExtender. NetExtender saves the information in a secure file on the smartphone.



Step 4 If One Time Password is enabled on the Dell SonicWALL SRA appliance, the One Time Password prompt is displayed. Enter the temporary password that was emailed to your configured account, and tap **OK**.

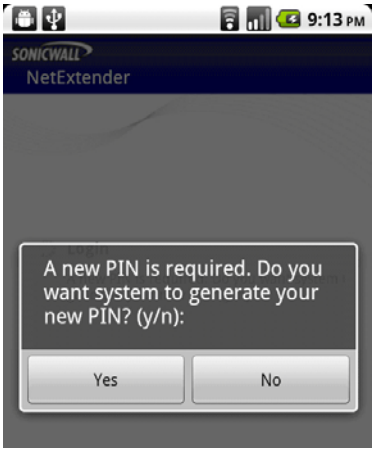


If your smartphone is synchronized to your email account, you can pull down the email notification from the top bar, or switch to your home page and access your email from there. After viewing the temporary password in your email or copying it to your clipboard, tap the NetExtender application icon to return directly to this screen.

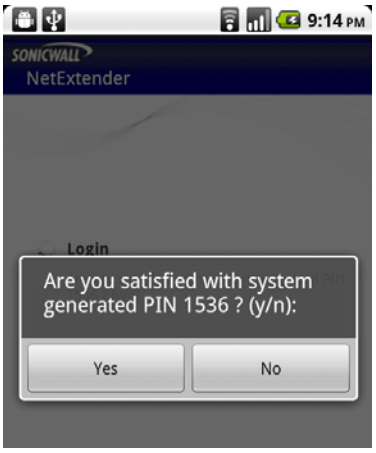
To use the clipboard, press the password in your email and select **Select Text**. Press the selected text again and select **Copy**. Then in the OTP screen, press the field and select **Paste**. Some Android smartphones require you to hold the **OK** button for clipboard access.

Step 5 If Two Factor Authentication is enabled on the Dell SonicWALL SRA appliance, you may be prompted to update your **PIN** (Personal Identification Number) or create a new one.

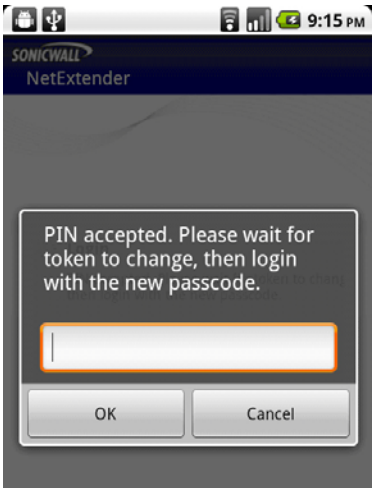
If no PIN has yet been configured, or if the administrator has reset the account, the following screen asks if the system should generate a new PIN. To allow the system to generate it, tap **Yes**. To type in a PIN yourself, tap **No** and skip to Step 7.



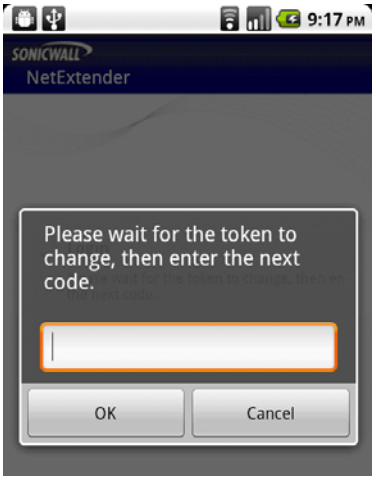
Step 6 If you chose to allow the system to generate the PIN, the display then prompts you to accept the generated PIN. Tap **Yes** to accept it, or tap **No** to have the system generate a different PIN. You are prompted each time until you tap **Yes**.



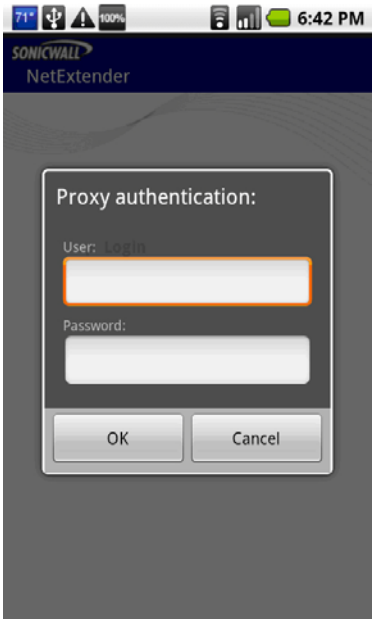
Step 7 If you chose to generate the PIN yourself, type a PIN into the PIN field and again in the second field to confirm it. Typically, PINs are required to be 4 to 8 digits. Tap **OK**.



Step 8 After entering the PIN or creating a new PIN, the Two Factor Authentication process requires you to enter the token code shown on your token device. Wait for the token code to change on the device, and then type the code into the field on your smartphone and tap **OK**.



Step 9 If a proxy server is configured in the smartphone (via Preferences), the Proxy Authentication screen is displayed next. Enter the username and password for the proxy and tap **OK**.

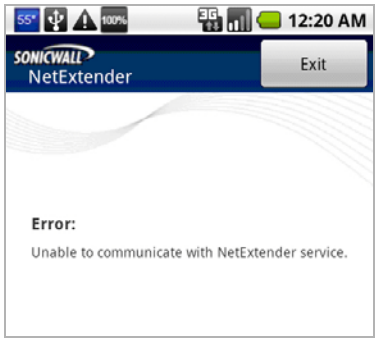


Step 10 NetExtender will connect at this point, unless there is a problem or error. You will see the NetExtender traffic indicator appear in the notification bar at the top of the display, unless it is disabled in Preferences.

The up and down arrows appear **white** when data is passing through the VPN tunnel. When no data is currently passing, the arrows appear **gray**. Control traffic does not affect the arrow colors.

The up arrow indicates that data is being sent from the smartphone to the network, and the down arrow indicates that data is being received from the network by the smartphone.

Step 11 If the NetExtender service running on the smartphone has a problem or has stopped running, the following screen is displayed. Tap **Exit** to quit the application. You may need to restart the service, possibly by turning the phone off and on again, or you may need to re-install NetExtender.



Exiting or Disconnecting from NetExtender

EXIT

Exiting and restarting NetExtender is useful when NetExtender cannot connect, possibly after a long period of disuse. To exit from NetExtender, perform the following steps:

Step 1 To access the **Exit** option, press the options or menu button while on the NetExtender screen. The options are displayed at the bottom of the screen.

Step 2 To cause NetExtender to exit completely, including the services component, select the **Exit** option and tap **OK**. You can restart NetExtender by clicking its icon on your smartphone.

DISCONNECT

To disconnect NetExtender, perform the following steps:

Step 1 Pull down the notification bar and click **NetExtender** to open the NetExtender user interface.

Step 2 In the NetExtender user interface, tap the **Disconnect** button and tap **OK** to confirm.

NetExtender notifies you while disconnecting.

Checking Status, Routes, and DNS Settings

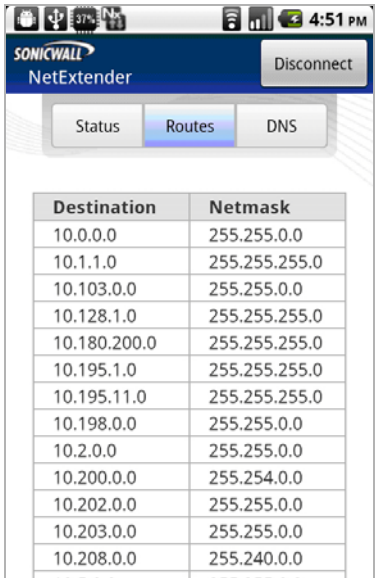
While NetExtender is connected, you can view status information, routes, and DNS settings on your smartphone.

Step 1 To open the NetExtender user interface, pull down the notification bar and tap **NetExtender**.

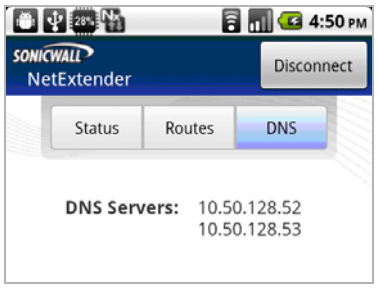
Step 2 To view status information, tap the **Status** tab. You can tap on the **Sent**, **Received**, or **Throughput** fields to change the units between bytes and packets.

If you are connected to a Dell SonicWALL SRA appliance running 5.0 or higher, and you have an Active Directory account, the **User** field contains your display name, such as "Sonia Eng". If you are connected to an appliance running the 4.0 release or you do not have an Active Directory account, the **User** field displays the login name, such as "seng".

Step 3 To view NetExtender routes, tap the **Routes** tab. The display shows all subnets currently available from the smartphone.



Step 4 To view the configured DNS servers, tap the **DNS** tab.



NetExtender Android supports DNS only; WINS or DNS suffix are not supported.

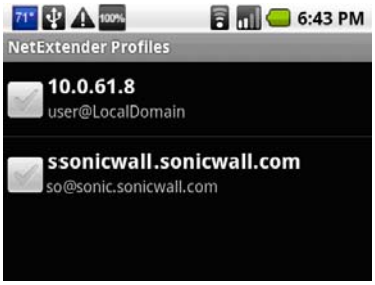
Configuring Profiles, Preferences, and Proxy Servers

To configure NetExtender profiles and preferences, including proxy servers, on your Android smartphone, perform the following steps:

Step 1 To display NetExtender options, start NetExtender and then press the options or menu button on the smartphone. The options are displayed at the bottom of the screen.

PROFILES

Step 2 To display the **NetExtender Profiles** screen, start NetExtender and then press the options or menu button on the smartphone and tap **Profiles**.



Step 3 To display the **Remove selected**, **Remove all**, and **Close** options on this **NetExtender Profiles** screen, press the options button while on the screen.

Step 4 Tap **Remove selected** to remove the profiles that have check marks next to them.

Step 5 Tap **Remove all** to remove all profiles from the smartphone.

Step 6 Tap **Close** to close the option display on this screen.

Step 7 To display the **Remove this profile, Remove selected profiles**, and **Remove all profiles** options, press and hold the **NetExtender Profiles** screen.

Step 8 Tap **Remove this profile** to remove the profile that you pressed on to bring up this screen.

Step 9 Tap **Remove selected** to remove the profiles that have check marks next to them.

Step 10 Tap **Remove all** to remove all profiles from the smartphone.

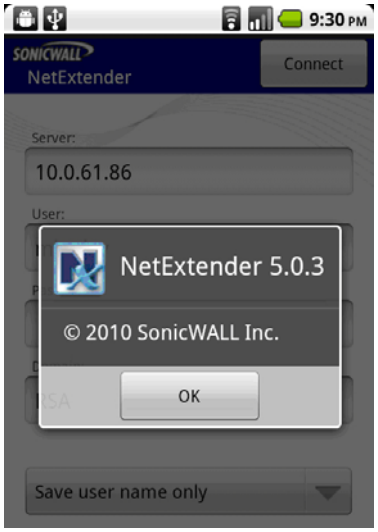
Step 11 Tap **Close** to close the option display on this screen.

EXPORT LOG

Step 12 To export the log file of NetExtender Android activity, select the **Export Log** option and enter the requested information.

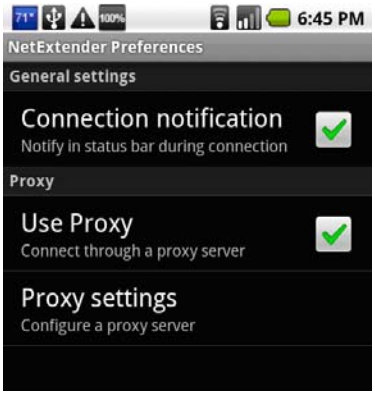
ABOUT

Step 13 To view NetExtender version information, select the **About** option.



PREFERENCES / PROXY SETTINGS

Step 14 To configure NetExtender preferences including proxy and notification settings, select the **Preferences** option.



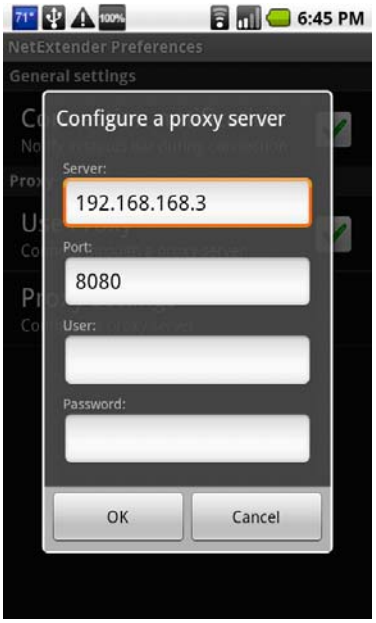
Step 15 Under **General settings**, select the **Connection notification** check box to display the NetExtender traffic indicator in the notification bar.

Clear the check box to prevent the indicator from being displayed.

Step 16 Under **Proxy**, select the **Use Proxy** check box to configure NetExtender Android to access external networks through a proxy server.

A proxy server is often used for access to the Internet if the initial connection is made to a local zone, such as LAN or WLAN.

Step 17 After selecting the **Use Proxy** check box, tap **Proxy settings** to open the configuration screen for the proxy server.



Step 18 Type the IP address of the proxy server into the **Server** field. Type the port number of the port that the server listens on into the **Port** field. This field displays “8080” by default, but there is no standard listening port for a proxy server.

Step 19 Optionally enter your login credentials for the server in the **User** and **Password** fields. Entering your credentials here causes NetExtender to save them, so that you can automatically connect to the proxy server during subsequent logins without being prompted for credentials.

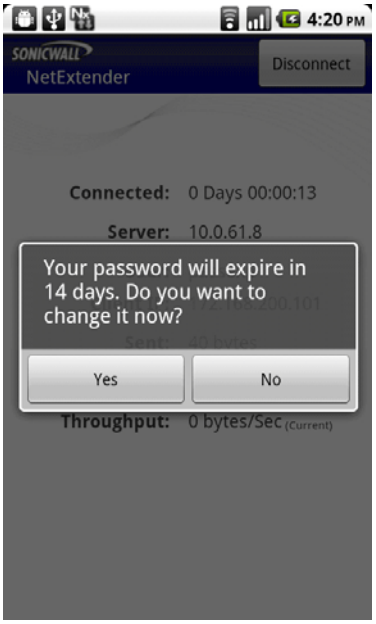
NetExtender Android supports basic authentication using a username and password for proxy servers. Microsoft NTLM authentication is not currently supported.

Step 20 When finished configuring the proxy server settings, tap **OK**.

Changing Your Password

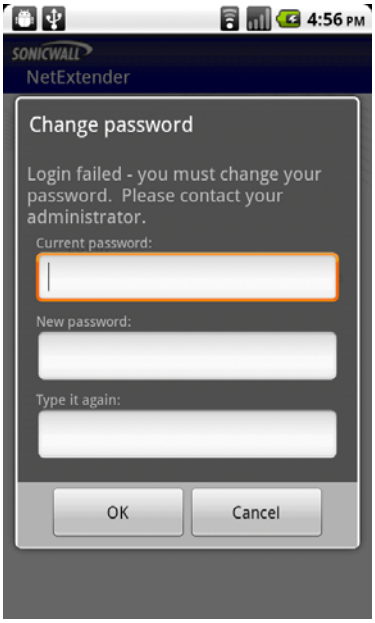
To change your password when prompted by NetExtender, perform the following steps:

Step 1 After connecting, a password expiration notice may be displayed on your Android smartphone. Tap **Yes** to change your password, or **No** to delay until a later time. NetExtender will remind you each time you connect.



Step 2 If you select **Yes**, the **Change password** screen is displayed. Type your password into the **Current Password** field, then type a new password into the **New password** field and again into the **Type it again** field. Tap **OK**.

Step 3 If your password expires before you change it, the **Change password** screen is displayed when you connect, with the message “Login failed – you must change your password.”



Type your old password into the **Current Password** field, then type a new password into the **New password** field and again into the **Type it again** field. Tap **OK**.

Related Documents

The following Technical Notes provide more information on advanced NetExtender scenarios:

- Running NetExtender on a Different TCP Port:
  http://www.sonicwall.com/us/support/2134_3154.html
- Using the Dell SonicWALL CDP Agent over a Dell SonicWALL NetExtender Connection
  http://www.sonicwall.com/us/support/2134_3487.html
- Using Dell SonicWALL NetExtender to Access FTP Servers
  http://www.sonicwall.com/us/support/2134_3465.html
- Resolving NetExtender Error With McAfee Enterprise 8.5
  http://www.sonicwall.com/us/support/2134_6813.html

Using Secure Virtual Assist

Secure Virtual Assist is an easy to use tool that allows Dell SonicWALL SSL VPN users to remotely support customers by taking control of their computers while the customer observes. Secure Virtual Assist is a lightweight, thin client that installs automatically using the Dell SonicWALL SSL VPN Virtual Office. Secure Virtual Assist can also be installed as a standalone client that can be launched directly from the client’s computer.

The following sections describe how to use Secure Virtual Assist:

- “Understanding Secure Virtual Assist” section on page 78
- “Installing and Launching Secure Virtual Assist” section on page 79
- “Configuring Secure Virtual Assist Settings” section on page 80
- “Selecting a Secure Virtual Assist Mode” section on page 82

- “Launching a Secure Virtual Assist Technician Session” section on page 82
- “Performing Secure Virtual Assist Technician Tasks” section on page 83
- “Initiating a Secure Virtual Assist Session from the Customer View” section on page 90
- “Using Secure Virtual Assist” section on page 100
- “Using Secure Virtual Assist in Unattended Mode” section on page 101
- “Enabling a System for Secure Virtual Access” section on page 102
- “Using the Request Assistance Feature” section on page 103

Understanding Secure Virtual Assist

Secure Virtual Assist is fully supported on Windows platforms. Secure Virtual Assist is certified to work on Windows 7, Windows Vista and Windows XP. The Secure Virtual Assist client is also available for Linux and Mac OS.

Note When a user requests service as a customer, Virtual Assist can be run while connected to the system over an RDP session for Windows 7 and Windows Vista platforms; however, Virtual Assist over RDP will have a limited set of features.

There are two sides to a Virtual Assist session: the customer view and the technician view. The customer is the person requesting assistance on their computer. The technician is the person providing assistance. A Virtual Assist session consists of the following sequence of events:

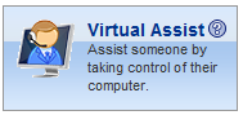
1. The technician launches Virtual Assist from the Dell SonicWALL SSL VPN Virtual Office.
2. The technician monitors the Assistance Queue for customers requesting assistance.
3. The customer requests assistance by one of these methods:
   - Logs into the Dell SonicWALL SSL VPN Virtual Office and clicks on the Virtual Assist link.
   - Receives an email invitation from the technician and clicks on the link to launch Virtual Assist.
   - Navigate directly to the URL of the Virtual Assist home page that is provided by the technician.
4. The Secure Virtual Assist application installs and runs on the customer’s system.
5. The customer appears in the Virtual Assist Assistance Queue.
6. The technician clicks on the customers name and launches a Virtual Assist session.
7. The technician’s Virtual Assist window now displays the customers entire display. The technician has complete control of the customer computer’s mouse and keyboard. The customer sees all of the actions that the technician performs.
8. If at anytime the customer wants to end the session, they can take control and click on an **End Virtual Assist** button in the bottom right corner of the screen.
9. When the session ends, the customer resumes sole control of the computer.

Installing and Launching Secure Virtual Assist

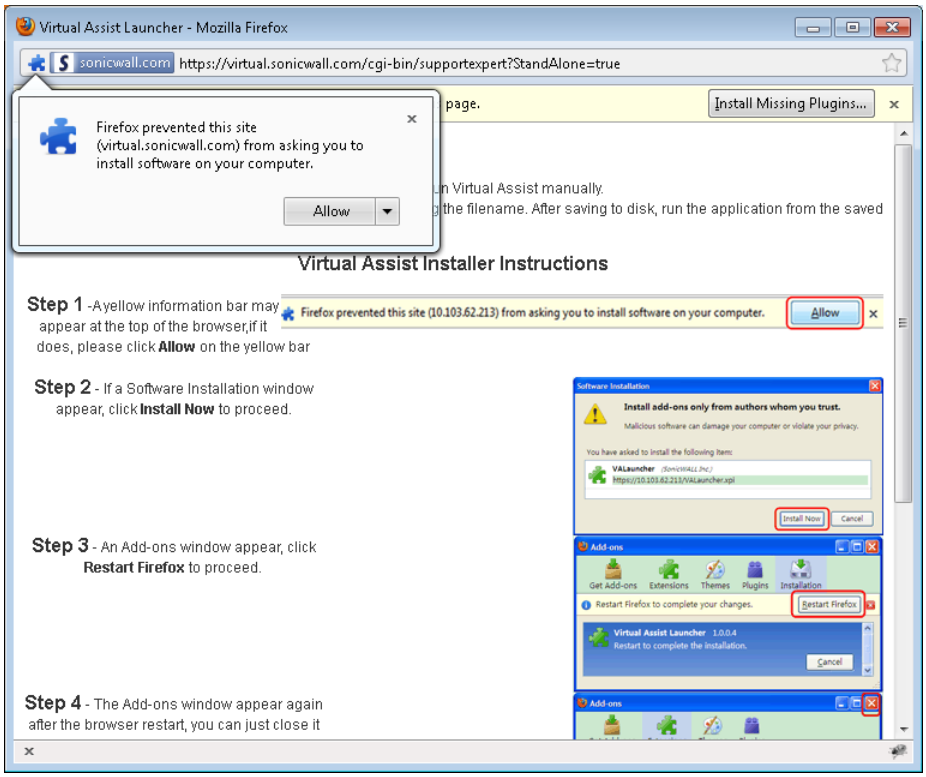
To install and launch a Virtual Assist session, perform the following steps.

Step 1 Log in to the Dell SonicWALL SRA security appliance Virtual Office. If you are already logged in to the Dell SonicWALL SSL VPN customer interface, click on the **Virtual Office** button.

Step 2 Click on the **Virtual Assist** button.

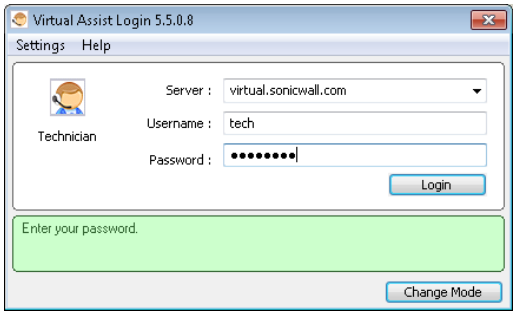


Step 3 The first time you launch Virtual Assist, you will be prompted to install the Secure Virtual Assist plugin and client.


Virtual Assist Launcher - Mozilla Firefox
sonicwall.com https://virtual.sonicwall.com/cgi-bin/supportexpert?StandAlone=true
Firefox prevented this site (virtual.sonicwall.com) from asking you to install software on your computer.
Allow
page.
Install Missing Plugins...
n Virtual Assist manually.
the filename. After saving to disk, run the application from the saved
Virtual Assist Installer Instructions
Step 1 -A yellow information bar may appear at the top of the browser,if it does, please click Allow on the yellow bar
Firefox prevented this site (10.103.62.213) from asking you to install software on your computer.
Allow
Step 2 - If a Software Installation window appear, click Install Now to proceed.
Step 3 - An Add-ons window appear, click Restart Firefox to proceed.
Step 4 - The Add-ons window appear again after the browser restart, you can just close it

Step 4 Click on the **Allow** button. A plugin installation window displays. Click **Install Now**. The Secure Virtual Assist plugin and client installs. You may be prompted to restart your browser.

Step 5 You can now launch Virtual Assist either from the Virtual Office window or from a shortcut that is added your Programs list under Window's start button.

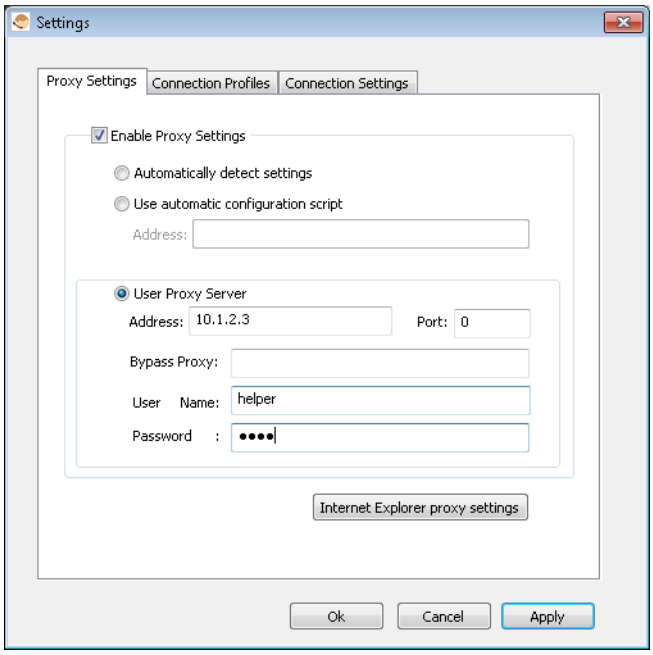


Configuring Secure Virtual Assist Settings

The Secure Virtual Assist Settings window can be accessed either by clicking the **Settings** button in the top left corner of the application window or by right-clicking on the Virtual Assist icon in the taskbar and selecting **Settings**.

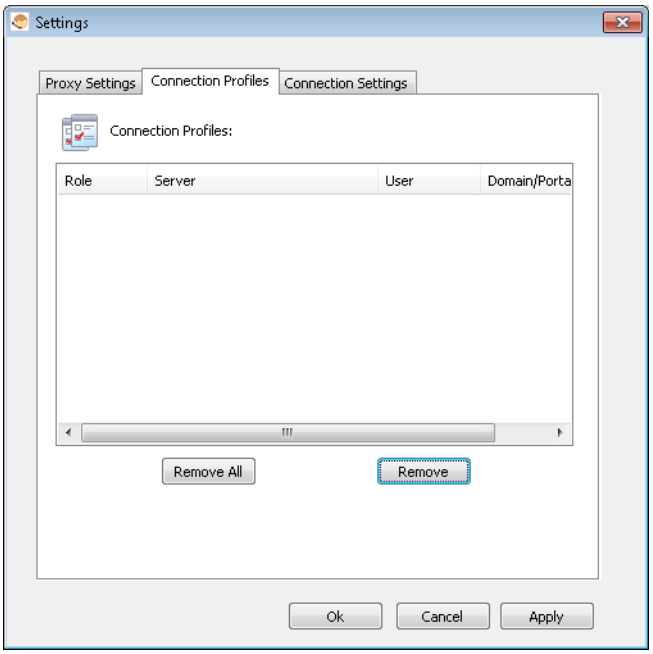
The Virtual Assist Settings window has three panes:

- **Proxy Settings** - Allows users to configure a Proxy server to access the SRA appliance. There are three options for configuring proxy settings.

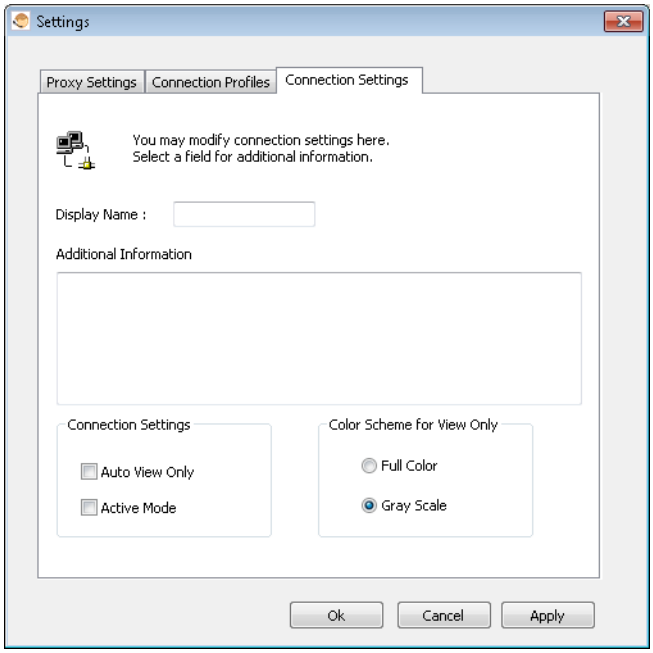


  - **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)), which can push the proxy settings script to the client automatically.
  - **Use automatic configuration script** - If you know the location of the proxy settings script, select this option and enter the URL of the scrip in the Address field.
  - **Use proxy server** - Select this option to enter the **Address** and **Port** of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses that bypass the proxy server. If required, enter a **User name** and **Password** for the proxy server. If the proxy server requires a username and password, but you do not specify them in the **Properties** window, a NetExtender pop-up window will prompt you to enter them when you first connect.
  - Optionally, you can click the **Internet Explorer proxy settings** button to open Internet Explorer's proxy settings page.

- **Connection Profiles** - Displays all of the Virtual Assist connection profiles that have been used on this computer. To remove a profile, select it and click the **Remove** button.



- **Connection Settings** - Allows users to customize how they are identified in Virtual Assist and the default settings of Virtual Assist customer sessions.

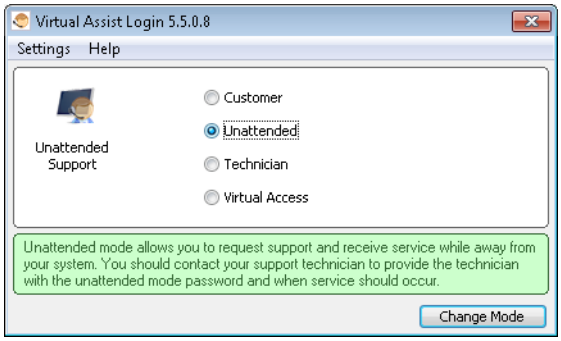


  - **Display Name** - The name that will be displayed in the user queue. By default, the users SSL VPN username is displayed.
  - **Additional Information** - Optional field to provide additional information.
  - **Auto View Only** - Specifies that Virtual Assist sessions will initially launch in View-Only mode instead of Trusted mode, which is the default.
  - **Active Mode** - Specifies that Virtual Assist sessions will initially launch in Active mode instead of Trusted mode, which is the default.

Selecting a Secure Virtual Assist Mode

When you first launch Secure Virtual Assist, by default it will be in customer mode. To change the mode, perform the following steps.

Step 1 Click **Change Mode** to select one of four possible modes.


Virtual Assist Login 5.5.0.8
Settings
Help
Unattended Support
Customer
Unattended
Technician
Virtual Access
Unattended mode allows you to request support and receive service while away from your system. You should contact your support technician to provide the technician with the unattended mode password and when service should occur.
Change Mode

Step 2 Select one of the following four Virtual Assist modes:

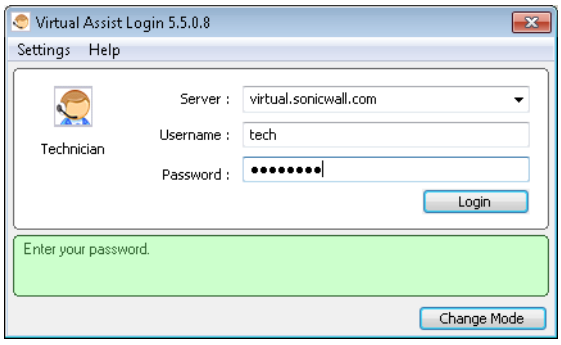
- **Customer** - Select this mode to request support. For information on customer mode, see the "Initiating a Secure Virtual Assist Session from the Customer View" section on page 90.
- **Unattended** - Select this mode to receive support help while you are away from your computer. You will be prompted to enter a password, which the technician can then enter and assume control of your system without further confirmation from you. For information on unattended mode, see the "Using Secure Virtual Assist in Unattended Mode" section on page 101.
- **Technician** - Select this mode to service customers by remotely controlling their systems. For information on technician mode, see the "Launching a Secure Virtual Assist Technician Session" section on page 82.
- **Virtual Access** - Select this mode to make your computer remotely accessible at all times from the SSL VPN appliance. For information on Secure Virtual Access mode, see the "Enabling a System for Secure Virtual Access" section on page 102.

Step 3 Click **Change Mode** again to login with the selected mode.

Launching a Secure Virtual Assist Technician Session

To launch a Virtual Assist technician session to remotely assist customers, perform the following steps.

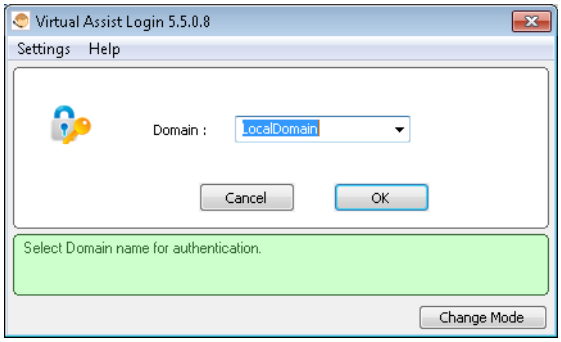
Step 1 Launch Virtual Assist and select the Technician Mode.



Step 2 In the **Server** drop-down menu, select the IP address or domain name of the Dell SonicWALL SRA appliance.

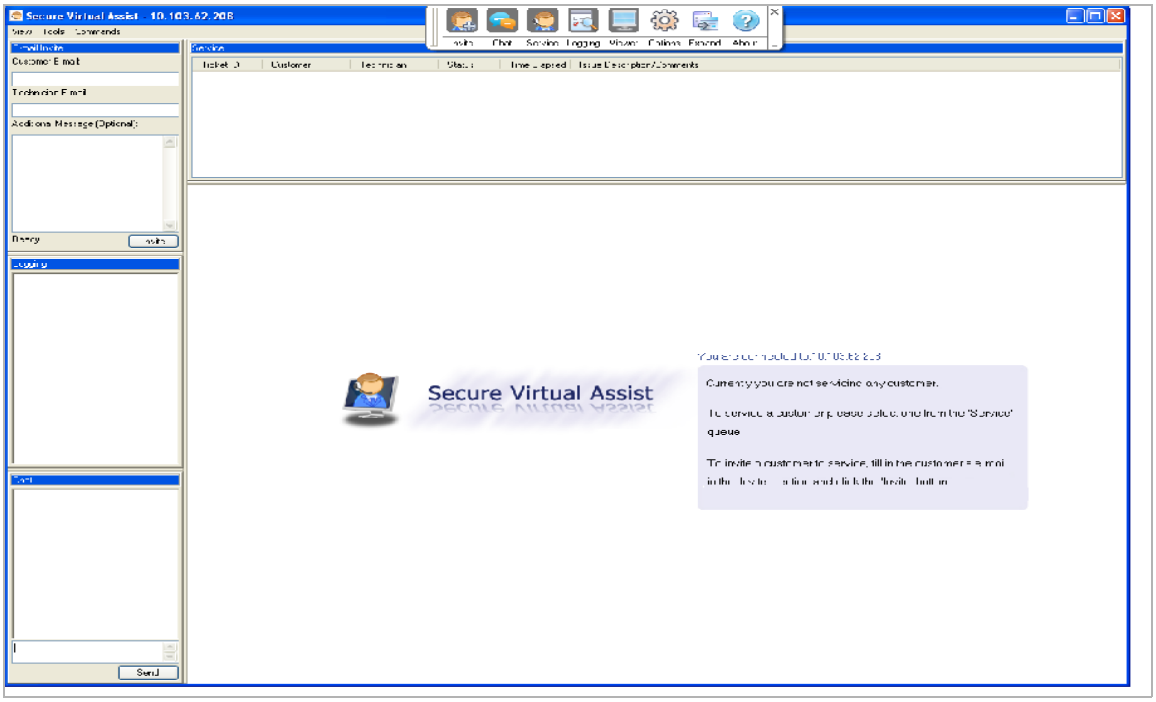
Step 3 Enter the **Username** and **Password** for the technician account on the appliance.

Step 4 Click **Login**.The Select Domain window displays.



Step 5 Select the **Domain** that the username is configured for and click **OK**.

Step 6 The Secure Virtual Assist standalone application launches.



The technician is now ready to assist customers.

Performing Secure Virtual Assist Technician Tasks

To get started, the technician logs into the Dell SonicWALL SRA appliance and launches the Secure Virtual Assist application.

Note Each technician can only assist one customer at a time.

By default, the Virtual Assist window launches with the Virtual Assist toolbar at the top and the rest of the window dedicated to the customer's screen.To display the most common panes, either click **Expand** or click **View > Classic Layout**. This will display the following panes:

- Email Invite
- Logging
- Chat
- Service

Once the technician has launched the Virtual Assist application, the technician can assist customers by performing the following tasks:

- "Inviting Customers by Email" on page 84
- "Assisting Customers" on page 85
- "Using the Virtual Assist Taskbar and Tab Controls" on page 86
- "Using the Secure Virtual Assist File Transfer" on page 89
- "Changing the Secure Virtual Assist Level of Control" on page 100
- "Ending a Virtual Assist Session" on page 101

Inviting Customers by Email

Step 1 To invite a customer to Virtual Assist, use the email invitation form on the left of the Virtual Assist window. If it is not displayed, click the **Invite** button in the toolbar.

Note Customers who launch Virtual Assist from an email invitation can only be assisted by the technician who sent the invitation. Customers who manually launch Virtual Assist can be assisted by any technician.

Step 2 Enter the customer's email address in the **Customer Email** field.

Step 3 Optionally, enter **Technician Email** to use a different return email address than the default technician email. Some mail servers require that an email address be entered, and that it be on a valid domain.

Step 4 Optionally, enter an **Additional Message** to the customer.

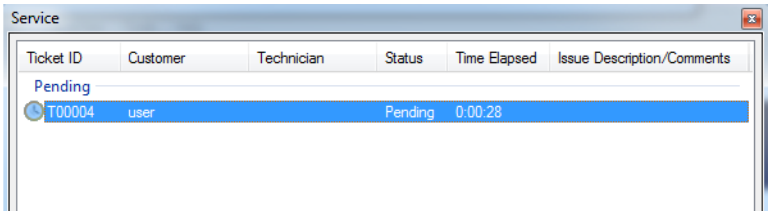
Step 5 Click **Invite**. The customer will receive an email with an HTML link to launch Virtual Assist.

Customers requesting assistance will appear in the Assistance Queue, and the duration of time they have been waiting will be displayed.

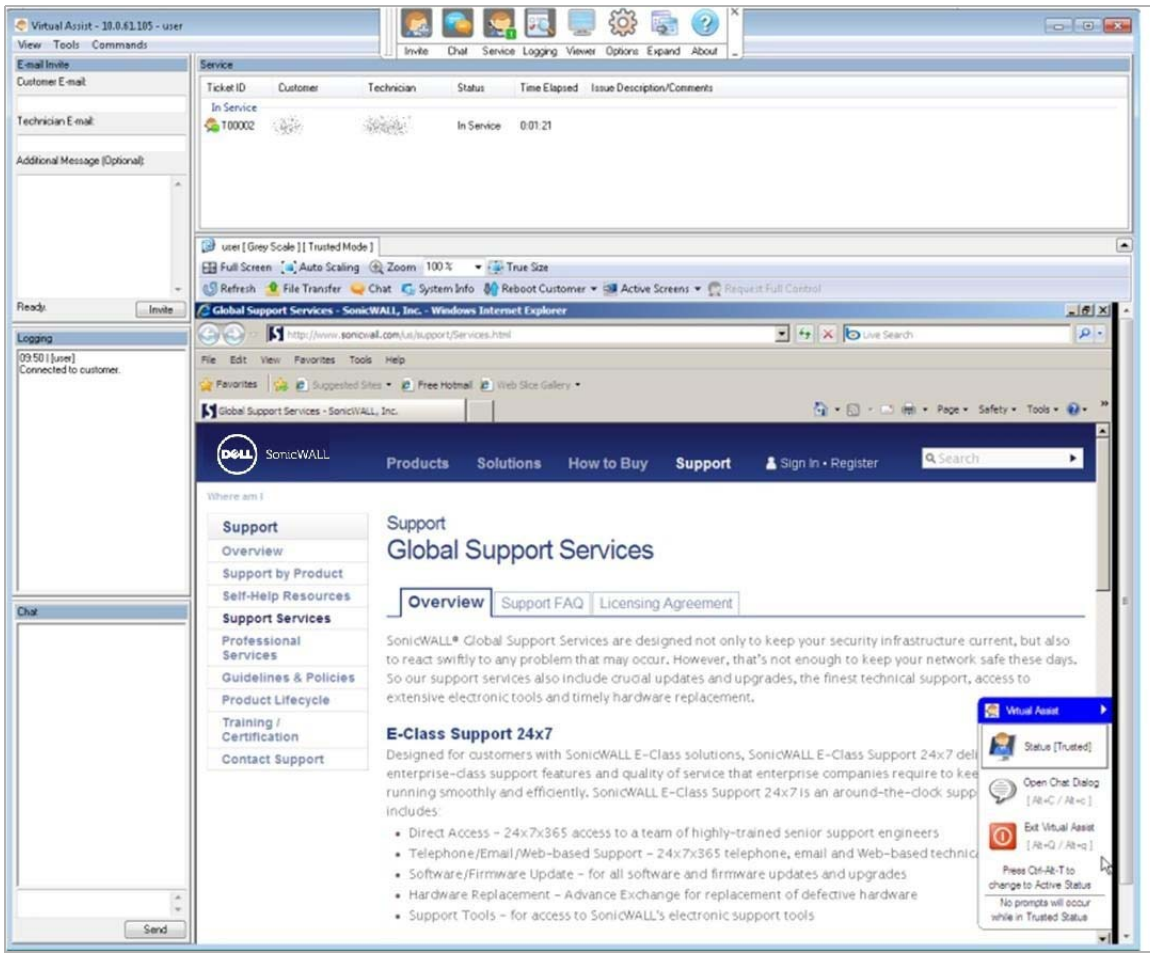
Assisting Customers

A pop-up window in the bottom right task bar alerts the technician when a customer is in the assistance queue. The customer queue is also displayed in the Service window.

Step 1 Double-click on a customer's user name to begin assisting the customer.



Step 2 The customer's entire desktop is displayed in the bottom right window of the Secure Virtual Assist application.



The technician now has complete control of the customer's keyboard and mouse. The customer can see all of the actions that the technician performs.

During a Virtual Assist session, the customer is not locked out of their computer. Both the technician and customer can control the computer, although this may cause confusion and consternation if they both attempt "to drive" at the same time.

The small tool bar in the bottom right of their screen provides three options during a Virtual Assist session:

- **Trusted/Active** - Toggles to the **View Only** mode, where the technician can view the customer's computer but cannot control the computer.
- **Chat** - Initiates a chat window with the technician.
- **End Virtual Assist** - Terminates the session.

Using the Virtual Assist Taskbar and Tab Controls

The Technician's view of Virtual Assist includes a Taskbar with a number of options.

- **Invite** - Displays the Email Invite pane.
- **Chat** - Displays the chat window to communicate with the customer.
- **Service** - Displays the service queue of customers awaiting service.
- **Logging** - Displays the log window.
- **Viewer** - Displays or hide the entire Virtual Assist window.
- **Options** - Displays Connection Profile and Connection Settings options.
- Expand - Displays the Email Invite, Service, Logging, and Chat panes.
- About - Displays the version information for the Secure Virtual Assist client.

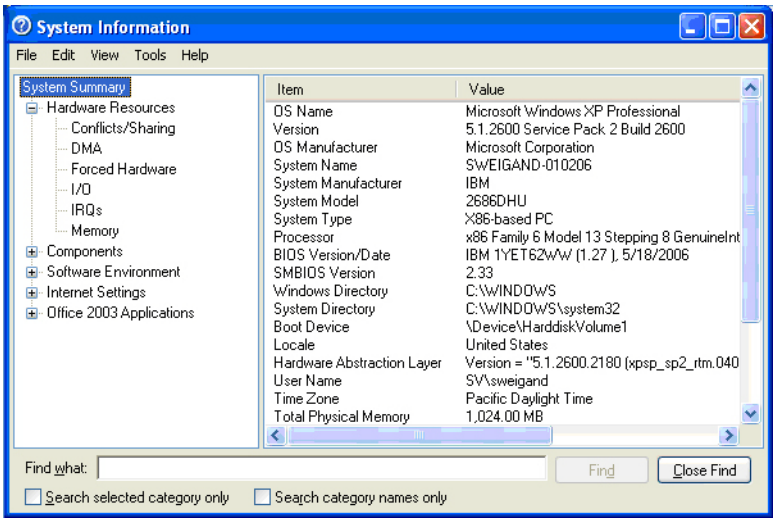
Note Clicking the _ button in the bottom right corner of the Taskbar will minimize the view so only the titles of the buttons are displayed, and not the icons. Clicking the **x** button in the top right of the corner will close Virtual Assist.

You can also display additional shortcuts and controls by selecting **View > Tab Controls for Current Customer**.

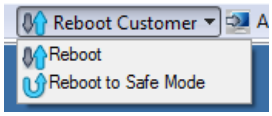
The following options appear at the top of the Virtual Assist window.

- **Full Screen** - Expands the Virtual Assist window to the technicians entire monitor.
- **Auto Scaling** - Fits the customer's screen to the Virtual Assist window.
- **Zoom** - Customizes the zoom of the customer's screen.
- **True Size** - Zooms to the actual size of the customer's monitor resolution.
- Gray Scale - Change the display to gray scale instead of full color.
- **Refresh** - Refreshes the customer's screen.
- **File Transfer** - Opens the File Transfer utility. See the "Using the Secure Virtual Assist File Transfer" on page 89 for more information.
- **Chat** - Opens a chat window with the customer.

- **System Info** -Provides detailed information to the technician about the customer's computer.



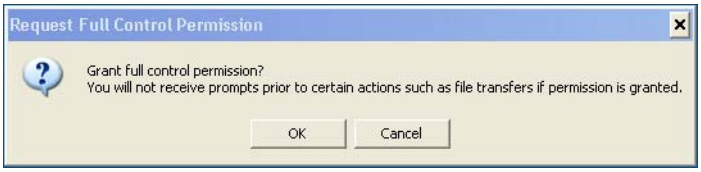
- **Reboot Customer** - Reboot the customer's computer. Unless you have Requested full control, the customer will be warned about and given the opportunity to deny the reboot. You can select either a basic reboot or to reboot into Safe Mode with Networking.



Note When rebooting, you will be prompted to enter the login credentials for the computer.

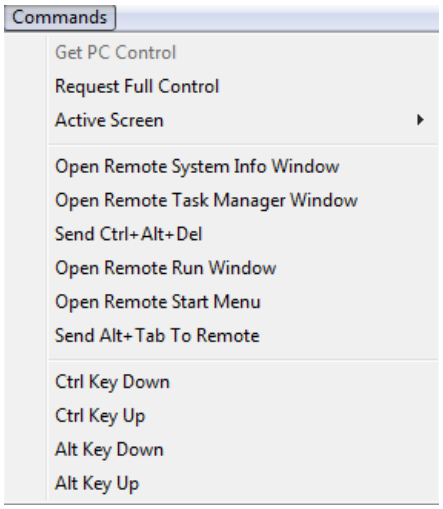
Reboot Authentication
Please enter in your Login Credentials for automatic login after reboot. Be sure the information is correct or the reboot process will be interrupted.
Note: Some Registery changes will be made, please allow all changes.
User Name:
user
Password:
Domain:
XPVM1
OK
Cancel

- **Active Screens** - Allows the technician to switch to a second monitor if the customer's computer has more than one monitor configured, or display all monitors.
- **Request Full Control** - Technicians can request full control of a customer's desktop, allowing them to reboot the system, delete files, or over-write files on the customer's computer without the customer being repeatedly prompted for permission. Select Request Full Control under the Commands menu to issue a request that will appear on the customer's desktop.


Request Full Control Permission
Grant full control permission?
You will not receive prompts prior to certain actions such as file transfers if permission is granted.
OK
Cancel

Using Additional Secure Virtual Assist Technician Commands

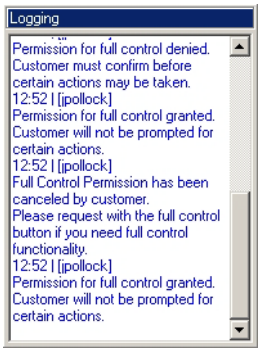
The **Commands** drop-down menu in the top left of the Virtual Assist window provides access to several of the options described above along with additional options.



- Open Remote System Info Window - Opens the System Info Window on the customer's computer.
- **Open Remote Task Manager Window** - Opens the Task Manager on the customer's computer.
- **Send Ctrl+Alt+Del** - Enters Control-Alt-Delete on the customer's computer.
- **Open Remote Run Menu** - Opens the Run menu on the customer's computer.
- **Open Remote Start Menu** - Opens the Start menu on the customer's computer.
- **Send Alt+Tab to Remote** - Enters Alt-Tab on the customer's computer to toggle between open windows.
- **Ctrl Key Down** - Engages the Control key on the customer's computer.
- **Ctrl Key Up** - Disengages the Control key on the customer's computer.
- **Alt Key Down** - Engages the Alt key on the customer's computer.
- **Alt Key Up** - Disengages the Alt key on the customer's computer.

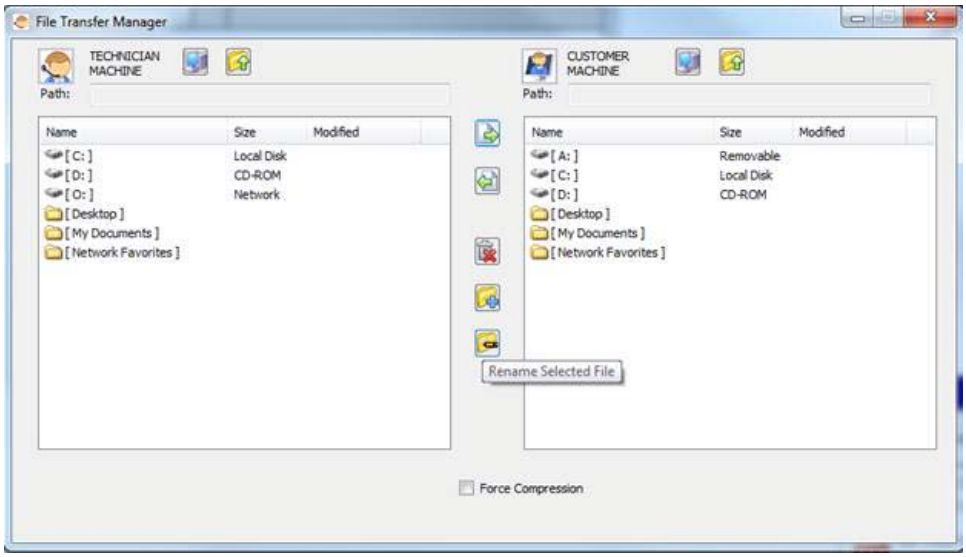
Viewing Secure Virtual Assist Session Log

The Secure Virtual Assist Session Log window can be displayed by clicking the **Logging** button in the Taskbar. The log displays a history of timestamped events for the session, such as opening Chat or File Transfer, requesting Full Control, etc.


Logging
Permission for full control denied.
Customer must confirm before certain actions may be taken.
12:52 | [jpollock]
Permission for full control granted.
Customer will not be prompted for certain actions.
12:52 | [jpollock]
Full Control Permission has been canceled by customer.
Please request with the full control button if you need full control functionality.
12:52 | [jpollock]
Permission for full control granted.
Customer will not be prompted for certain actions.

Using the Secure Virtual Assist File Transfer

The File Transfer window is used to transfer files to and from the customer's computer. The file directory of the technician's computer is shown on the left and the customer's computer on the right.



The File Transfer window functions in much the same manner as Windows Explorer or an FTP program. Navigate the File Transfer window by double-clicking on folders and selecting files. The File Transfer window includes the following controls:

- **Desktop** jumps to the desktop of the technician's or customer's computer.
- **Up** navigates up one directory on either the technician's or customer's computer.
- **Download** transfers the selected file or files from the technician's computer to the customer's computer.
- **Upload** transfers the selected file or files from the customer's computer to the technician's computer.
- **Delete** deletes the selected file or files.

Note When deleting or overwriting files, the customer is warned and must give the technician permission unless the technician has clicked the **Request Full Control** button and the customer has confirmed.

- **New folder** creates a new folder in the selected directory.
- **Rename** renames the selected file or directory.

When a file is transferring, the transfer progress is displayed at the bottom of the File Transfer window. Click the **Exit** button to cancel a transfer in progress.

Note File Transfer supports the transfer of single or multiple files. It does not currently support the transfer of directories. To select multiple files, hold down the **Ctrl** button while clicking on the files.

Initiating a Secure Virtual Assist Session from the Customer View

The following sections describe how to use Virtual Assist on the three supported client platforms:

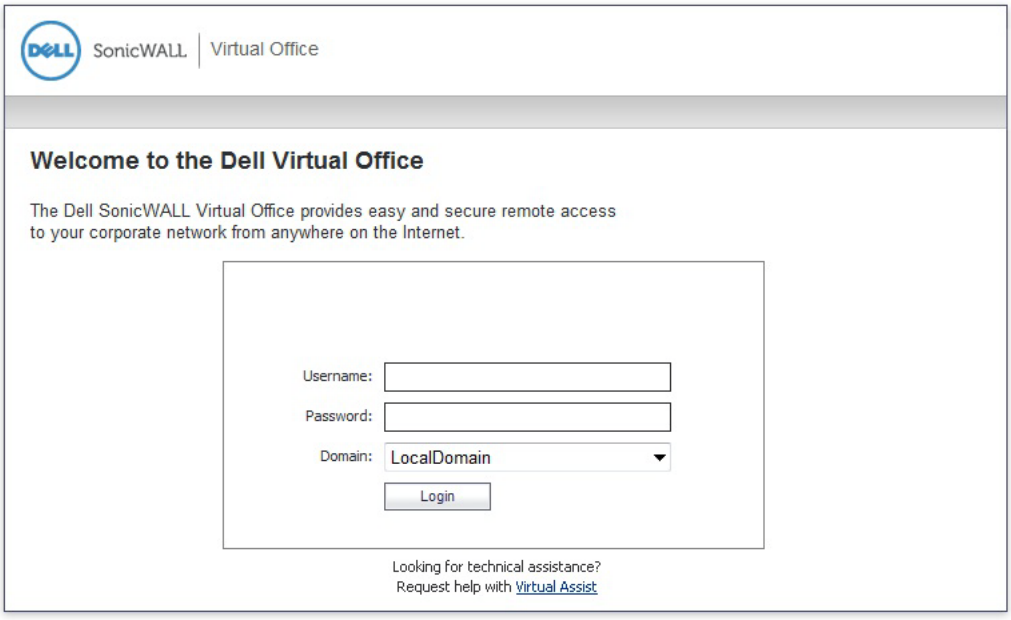
- “Initiating Secure Virtual Assist on a Windows Client” section on page 90
- “Initiating Secure Virtual Assist on a MacOS Client” section on page 93
- “Initiating Secure Virtual Assist on a Linux Client” section on page 97

Initiating Secure Virtual Assist on a Windows Client

To launch a Virtual Assist customer session to request help on your Windows computer, perform the following steps:

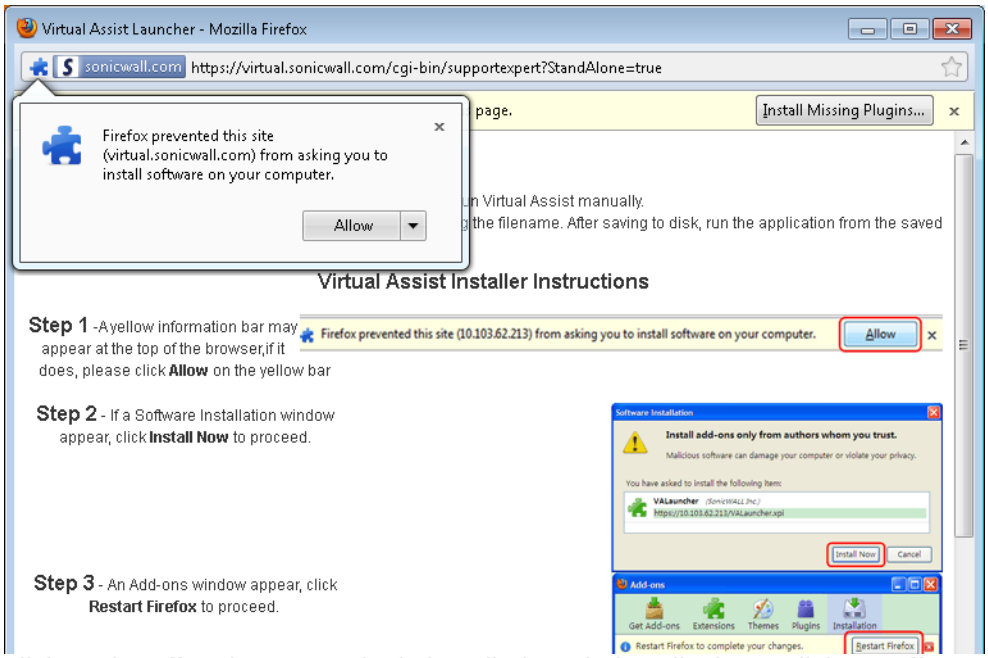
Step 1 There are several methods for accessing Virtual Assist:

- Navigate to the URL of the Virtual Assist home page that is provided by your support technician.
- If you received an email invitation, click on the link in the email or paste the URL into your Web browser.
- The login page of your Virtual Office may include a direct link to Virtual Assist as shown below.

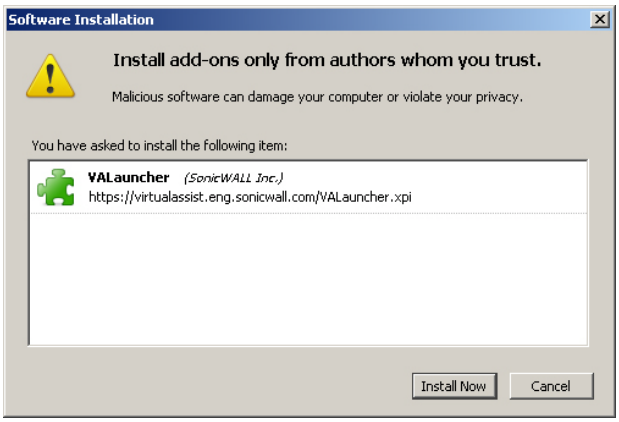


- Or you may need to login to the Virtual Office and click the **Request Assistance** button.

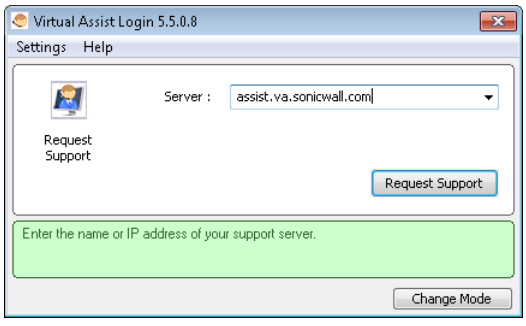
Step 2 The first time you launch Virtual Assist, you will be prompted to install the Secure Virtual Assist plugin and client.


Virtual Assist Launcher - Mozilla Firefox
sonicwall.com https://virtual.sonicwall.com/cgi-bin/supportexpert?StandAlone=true
Firefox prevented this site (virtual.sonicwall.com) from asking you to install software on your computer.
Allow
page.
Install Missing Plugins...
n Virtual Assist manually.
the filename. After saving to disk, run the application from the saved
Virtual Assist Installer Instructions
Step 1 -A yellow information bar may appear at the top of the browser,if it does, please click Allow on the yellow bar
Firefox prevented this site (10.103.62.213) from asking you to install software on your computer.
Allow
Step 2 - If a Software Installation window appear, click Install Now to proceed.
Step 3 - An Add-ons window appear, click Restart Firefox to proceed.

Step 3 Click on the **Allow** button. A plugin installation window displays. Click **Install Now**. The Secure Virtual Assist plugin and client installs. You may be prompted to restart your browser.


Software Installation
Install add-ons only from authors whom you trust.
Malicious software can damage your computer or violate your privacy.
You have asked to install the following item:
VALauncher (SonicWALL Inc.)
https://virtualassist.eng.sonicwall.com/VALauncher.xpi
Install Now
Cancel

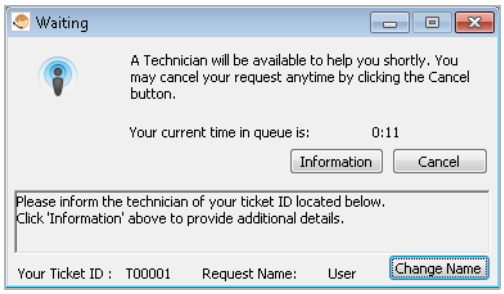
Step 4 You can now launch Virtual Assist either from the Virtual Office window or from a shortcut that is added your Programs list under Window's start button. If the **Server** address is not auto-propagated in the login window, enter the Server address and click **Request Support**. The server address can be either an IP address, IPv6 address, or hostname of the Dell SonicWALL SRA appliance. IPv6 addresses must be enclosed in brackets (the **[** and **]** symbols).



Step 5 If you receive the following security alert, click **Unblock** to allow Virtual Assist traffic through the Windows firewall.

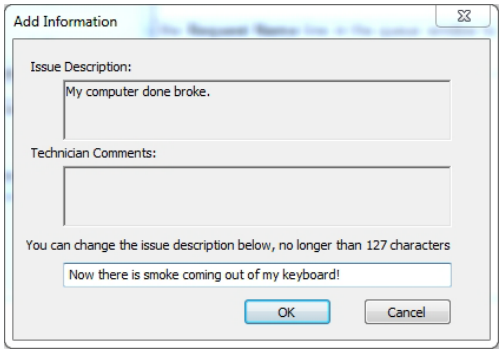
Windows Security Alert
To help protect your computer, Windows Firewall has blocked some features of this program.
Do you want to keep blocking this program?
Name: SWTunnel
Publisher: Unknown
Keep Blocking
Unblock
Ask Me Later
Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Step 6 A pop-up window indicates that you are in the Virtual Assist queue. The technician will be alerted that you are ready. Click **Cancel** to cancel the Virtual Assist request.

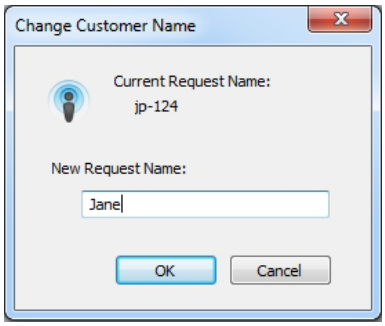

Waiting
A Technician will be available to help you shortly. You may cancel your request anytime by clicking the Cancel button.
Your current time in queue is: 0:11
Information
Cancel
Please inform the technician of your ticket ID located below.
Click 'Information' above to provide additional details.
Your Ticket ID : T00001
Request Name: User
Change Name

Step 7 The Virtual Assist queue window provides two options:

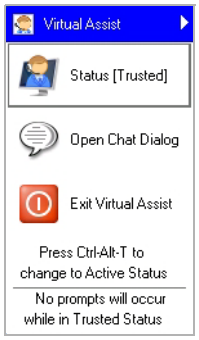
- Click the **information** to provide the technician with information about your issue.


Add Information
Issue Description:
My computer done broke.
Technician Comments:
You can change the issue description below, no longer than 127 characters
Now there is smoke coming out of my keyboard!
OK
Cancel

- Click the icon next to the **Change Name** line in the queue window to specify your name. By default, the computer name is used.



Step 8 When the technician initiates the session, the Virtual Assist toolbar appears in the bottom right of your screen. The technician now has control of your computer.


Virtual Assist
Status [Trusted]
Open Chat Dialog
Exit Virtual Assist
Press Ctrl-Alt-T to change to Active Status
No prompts will occur while in Trusted Status

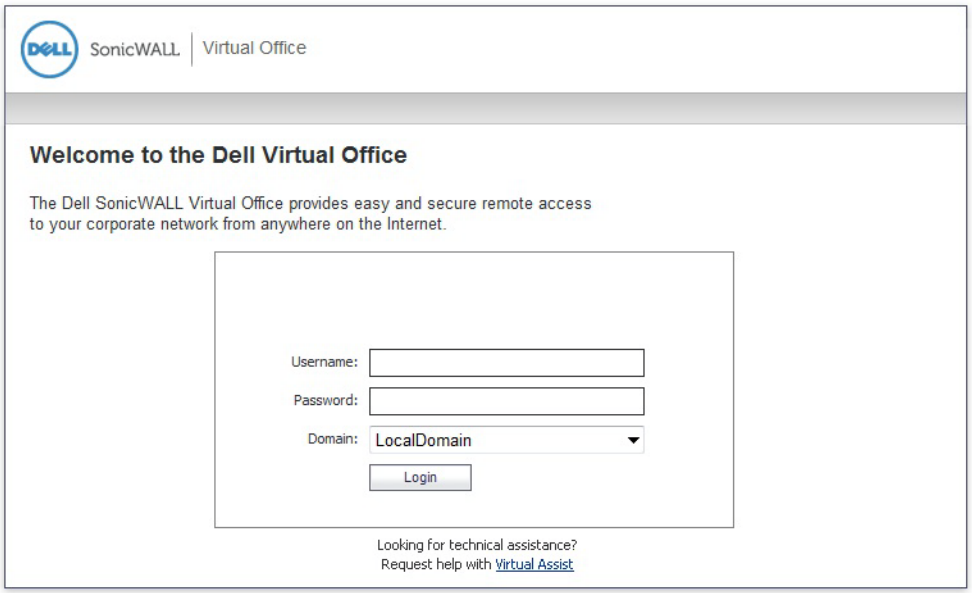
Step 9 For information on using Virtual Assist once the session is active, see "Using Secure Virtual Assist" section on page 100.

Initiating Secure Virtual Assist on a MacOS Client

To launch a Virtual Assist customer session to request help on your MacOS computer, perform the following steps:

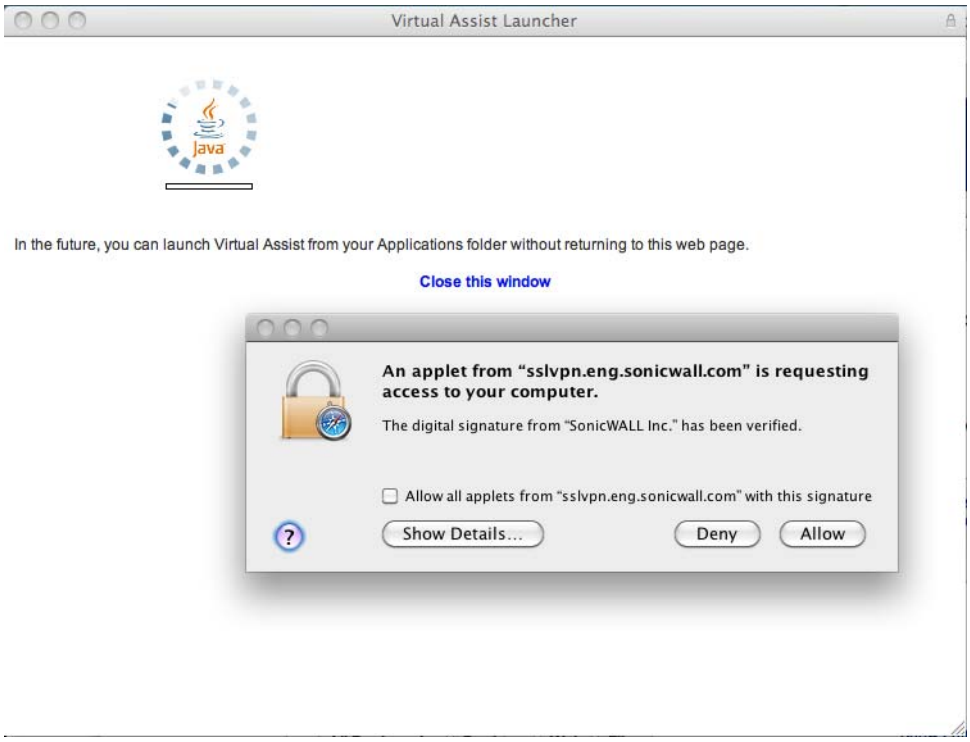
Step 1 There are several methods for accessing Virtual Assist:

- Navigate to the URL of the Virtual Assist home page that is provided by your support technician.
- If you received an email invitation, click on the link in the email or paste the URL into your Web browser.
- The login page of your Virtual Office may include a direct link to Virtual Assist as shown below.


SonicWALL | Virtual Office
Welcome to the Dell Virtual Office
The Dell SonicWALL Virtual Office provides easy and secure remote access to your corporate network from anywhere on the Internet.
Username:
Password:
Domain:
LocalDomain
Login
Looking for technical assistance?
Request help with Virtual Assist

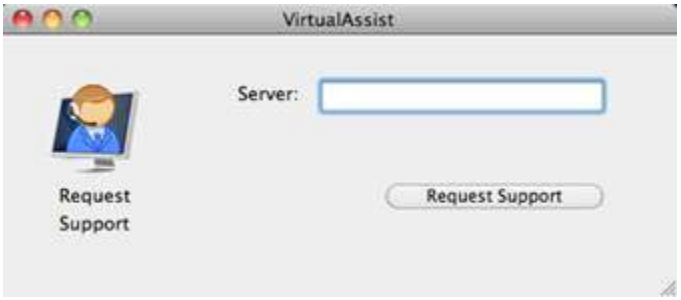
- Or you may need to login to the Virtual Office and click the **Request Assistance** button.

Step 2 The first time you launch Virtual Assist, you will be prompted to allow the Secure Virtual Assist applet to be installed on your computer. Click **Allow**.

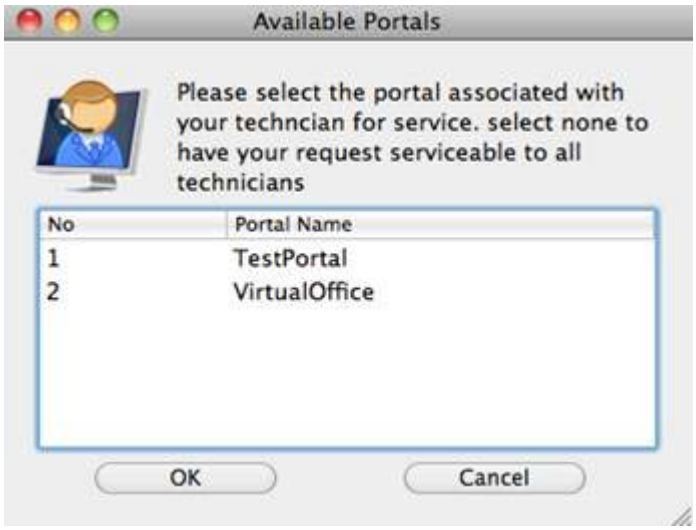

Virtual Assist Launcher
Java
In the future, you can launch Virtual Assist from your Applications folder without returning to this web page.
Close this window
An applet from "sslvpn.eng.sonicwall.com" is requesting access to your computer.
The digital signature from "SonicWALL Inc." has been verified.
Allow all applets from "sslvpn.eng.sonicwall.com" with this signature
Show Details...
Deny
Allow

Step 3 The Secure Virtual Assist client installs and launches. In the future, you can either launch Virtual Assist either by navigating to the Virtual Office window in your browser, or you can launch it directly from your Applications folder.

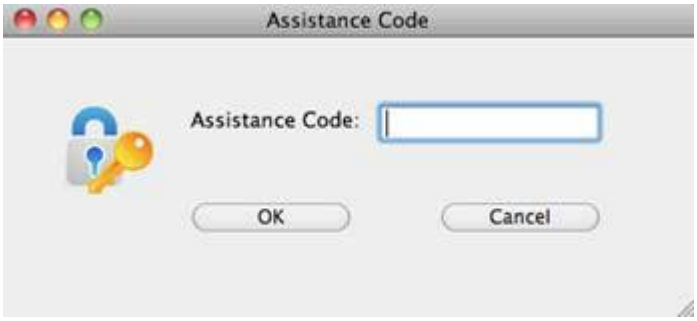
Step 4 If the **Server** address is not auto-propagated in the login window, enter the Server address and click **Request Support**. The server address can be either an IP address, IPv6 address, or hostname of the Dell SonicWALL SRA appliance. IPv6 addresses must be enclosed in brackets (the **[** and **]** symbols).



Step 5 The list of Available Portals is displayed. To connect to a specific portal, select it and click **OK**. To have your request be serviceable by all of the portals, click **OK** without selecting a specific portal.



Step 6 You may be prompted to enter an **Assistance Code**.



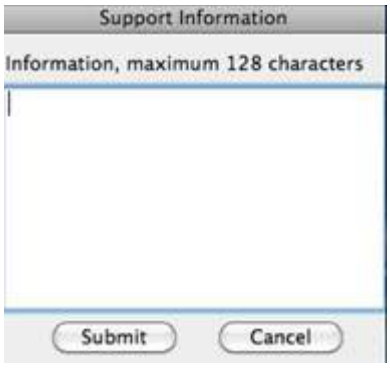
Step 7 You may be prompted to read and accept a disclaimer. Click **OK**.

Step 8 A pop-up window indicates that you are in the Virtual Assist queue. The technician will be alerted that you are ready. Click **Cancel** to cancel the Virtual Assist request.

Waiting
A technician will be available to help you shortly. You may cancel your request anytime by clicking the Cancel button.
Your current time in queue is: 0:24
Add Information
Cancel
Please inform the technician of your ticket ID located below.
Click 'Add Information' above to provide additional details
Your Ticket ID: T00020
Request Name: derek-y...

Step 9 The Virtual Assist queue window provides two options:

- Click **Add information** to provide the technician with information about your issue.



- Click the icon next to the **Request Name** line in the queue window to specify your name. By default, the computer name is used.

Step 10 When the technician initiates the session, the Virtual Assist toolbar appears in the bottom right of your screen. The technician now has control of your computer.

Virtual Assist
Status [Trusted]
Open Chat Dialog
End Support
Press Ctrl+Alt+T to change to Active Status
No Prompts will occur when in Trusted Status

Step 11 For information on using Virtual Assist once the session is active, see "Using Secure Virtual Assist" section on page 100.

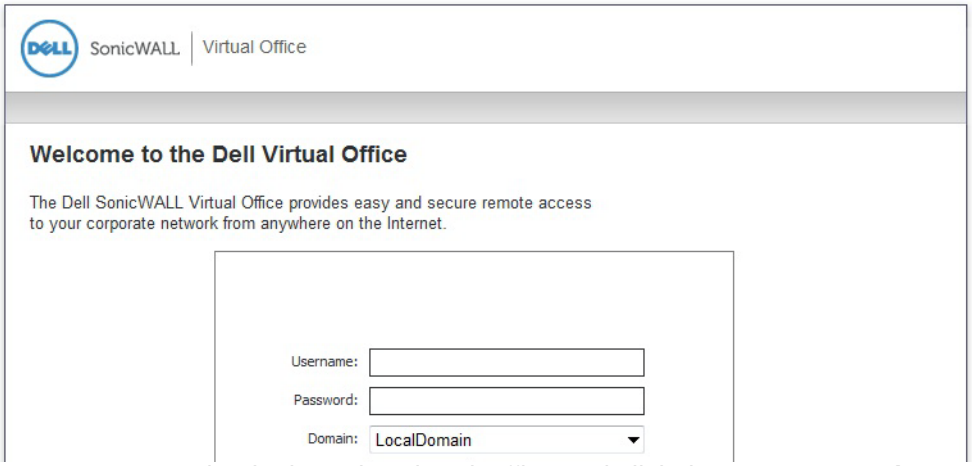
Initiating Secure Virtual Assist on a Linux Client

Note Dell SonicWALL Secure Virtual Assist is fully tested on the Ubuntu distribution of Linux. It has not been tested on other Linux distributions.

To launch a Virtual Assist customer session to request help on your Linux computer, perform the following steps:

Step 1 There are several methods for accessing Virtual Assist:

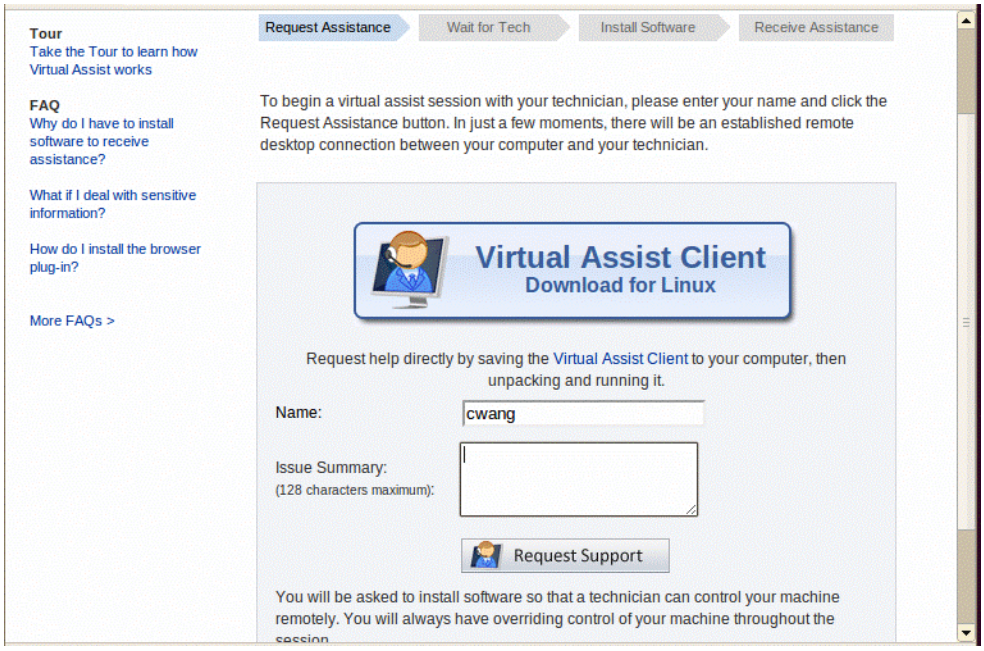
- Navigate to the URL of the Virtual Assist home page that is provided by your support technician.
- If you received an email invitation, click on the link in the email or paste the URL into your Web browser.
- The login page of your Virtual Office may include a direct link to Virtual Assist as shown below.


SonicWALL
Virtual Office
Welcome to the Dell Virtual Office
The Dell SonicWALL Virtual Office provides easy and secure remote access to your corporate network from anywhere on the Internet.
Username:
Password:
Domain:
LocalDomain

- Or you may need to login to the Virtual Office and click the **Request Assistance** button.

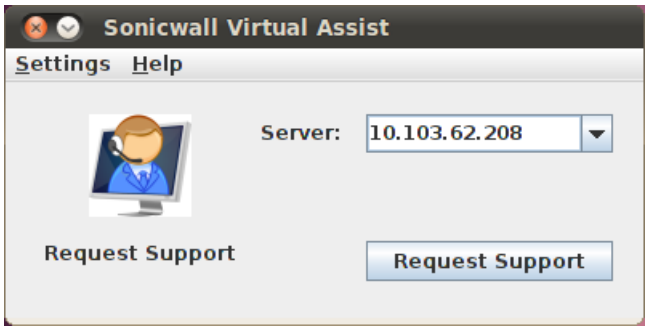
Step 2 You will be prompted to click the **Virtual Assist Client Download for Linux** button. It will prompt you to download the “VACLinux.x86.tgz” file. Unpackage the file and run the “Install” file. You can now launch Virtual Assist either from a shortcut on your desktop or by typing **VirtualAssistGui** in the Terminal window.

Step 3 Optionally, you can enter your name and a summary of your issue and click **Request Support**. You will then be prompted to install the Secure Virtual Assist client. After the installation is complete, the Secure Virtual Assist client will launch automatically.

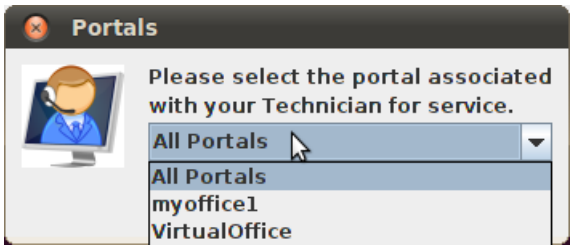

Tour
Take the Tour to learn how Virtual Assist works
FAQ
Why do I have to install software to receive assistance?
What if I deal with sensitive information?
How do I install the browser plug-in?
More FAQs >
Request Assistance
Wait for Tech
Install Software
Receive Assistance
To begin a virtual assist session with your technician, please enter your name and click the Request Assistance button. In just a few moments, there will be an established remote desktop connection between your computer and your technician.
Virtual Assist Client
Download for Linux
Request help directly by saving the Virtual Assist Client to your computer, then unpacking and running it.
Name:
cwang
Issue Summary:
(128 characters maximum):
Request Support
You will be asked to install software so that a technician can control your machine remotely. You will always have overriding control of your machine throughout the session

Step 4 You can now launch Virtual Assist either from a shortcut on your desktop or by typing **VirtualAssistGui** in the Terminal window.

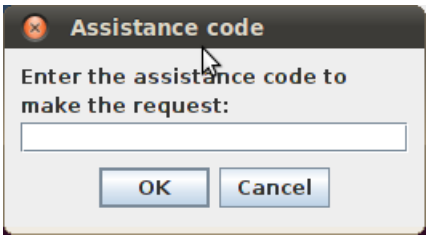
Step 5 If the **Server** address is not auto-propagated in the login window, enter the Server address and click **Request Support**. The server address can be either an IP address, IPv6 address, or hostname of the Dell SonicWALL SRA appliance. IPv6 addresses must be enclosed in brackets (the **[** and **]** symbols).



Step 6 The list of Available Portals is displayed. To connect to a specific portal, select it and click **OK**. To have your request be serviceable by all of the portals, select **All Portals** and click **OK**.

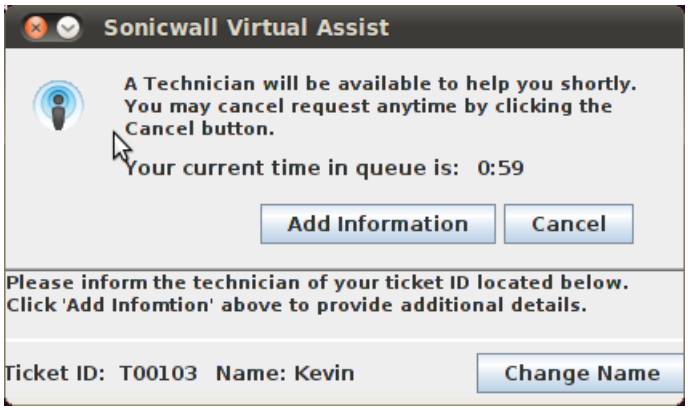


Step 7 You may be prompted to enter an **Assistance Code**.



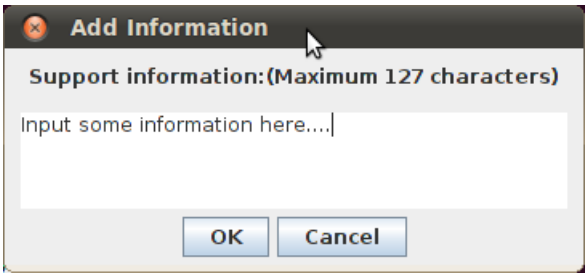
Step 8 You may be prompted to read and accept a disclaimer. Click **OK**.

Step 9 A pop-up window indicates that you are in the Virtual Assist queue. The technician will be alerted that you are ready. Click **Cancel** to cancel the Virtual Assist request.


Sonicwall Virtual Assist
A Technician will be available to help you shortly. You may cancel request anytime by clicking the Cancel button.
Your current time in queue is: 0:59
Add Information
Cancel
Please inform the technician of your ticket ID located below. Click 'Add Infomtion' above to provide additional details.
Ticket ID: T00103 Name: Kevin
Change Name

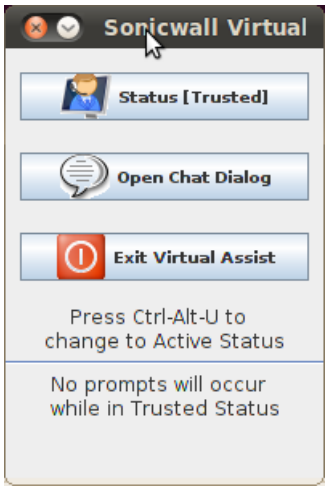
Step 10 The Virtual Assist queue window provides two options:

- Click **Add information** to provide the technician with information about your issue.



- Click the icon next to the **Request Name** line in the queue window to specify your name. By default, the computer name is used.

Step 11 When the technician initiates the session, the Virtual Assist toolbar appears in the bottom right of your screen. The technician now has control of your computer.


Sonicwall Virtual
Status [Trusted]
Open Chat Dialog
Exit Virtual Assist
Press Ctrl-Alt-U to change to Active Status
No prompts will occur while in Trusted Status

Step 12 For information on using Virtual Assist once the session is active, see "Using Secure Virtual Assist" section on page 100.

Using Secure Virtual Assist

During a Virtual Assist session, you are not completely locked out of your computer. Both the technician and customer can control the computer, although this may cause confusion and consternation if they both attempt to "drive" at the same time. You can resume control when the technician is not actively typing or moving the mouse. And you can end the session at any time by clicking the **End Virtual Assist** button in the bottom right corner.

Click the **Chat** button or enter **Alt-c** to open an instant message style chat session with the technician.

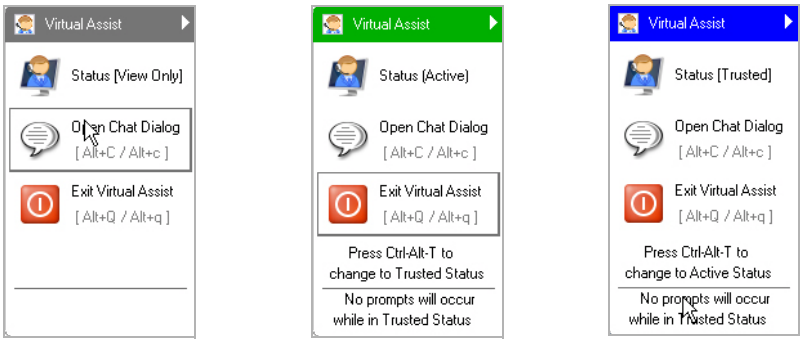
The technician can also open a Chat window to communicate with you. To chat, type text in the **Chat** window and type **Enter** or click **Send**.

Changing the Secure Virtual Assist Level of Control

There are three levels of control that a customer can grant to the technician:

- **View Only** - The technician can view the customer's computer but cannot control it. To switch to View Only mode, click the **Status (Active)** button. The Status switches to (View Only).
- **Active** - The technician can control the customer's computer, but the customer must give permission for certain action—such as allowing the technician to reboot the system, delete files, or over-write files on the customer's computer without the customer being repeatedly prompted for permission. To switch from View Only mode to Active mode, click the **Status (View Only)** button.

- **Trusted** - The technician has complete control of the customer's computer. To toggle between Trusted mode and Active mode, enter Ctrl-Alt-T.


Virtual Assist
Status [View Only]
Open Chat Dialog
[Alt+C / Alt+c]
Exit Virtual Assist
[Alt+Q / Alt+q]
Virtual Assist
Status [Active]
Open Chat Dialog
[Alt+C / Alt+c]
Exit Virtual Assist
[Alt+Q / Alt+q]
Press Ctrl-Alt-T to change to Trusted Status
No prompts will occur while in Trusted Status
Virtual Assist
Status [Trusted]
Open Chat Dialog
[Alt+C / Alt+c]
Exit Virtual Assist
[Alt+Q / Alt+q]
Press Ctrl-Alt-T to change to Active Status
No prompts will occur while in Trusted Status

Note By default, Virtual Assist sessions are launched in Trusted mode. To modify this, click the **Settings** button on the top left corner of the window, select the **Connection Settings** tab and select either **Auto View Only** or **Active Mode**.

Ending a Virtual Assist Session

You can end the Virtual Assist session at anytime by clicking on the **Exit Virtual Assist** button in the bottom right corner of the screen, or by entering **Alt-q**. This will end the technician's control of your computer.

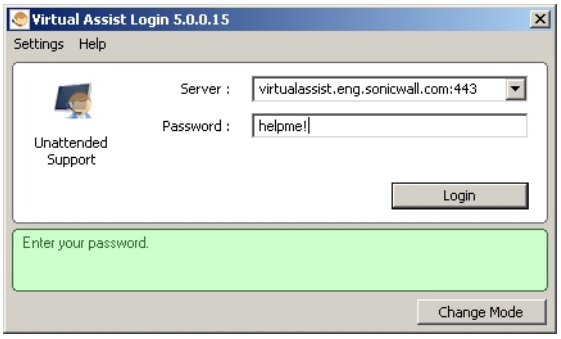
Using Secure Virtual Assist in Unattended Mode

Note Unattended Mode is supported only on Windows clients.

Unattended Mode allows customers to set their computer to be accessible by a technician at a later time when the customer will not be available to click to confirm their consent. To set your computer for Secure Virtual Assist Unattended Mode, perform the following tasks:

Step 1 Launch Virtual Assist.

Step 2 Click **Change Mode**, select **Unattended**, and click **Change Mode** again.



Step 3 Select or enter the IP address or domain name of the SSL VPN server.

Step 4 Enter a **Password** and click **Login**. The Waiting window displays and shows the length of time you have been in the queue.

Step 5 You need to provide the technician with the password you just defined. An easy way to do this is to click **Add Information** and give the technician your password.

Enabling a System for Secure Virtual Access

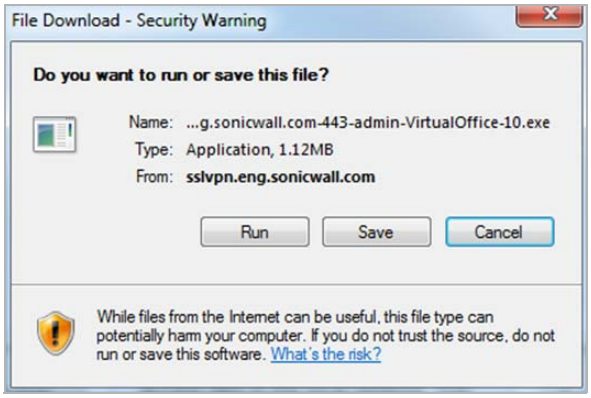
Note Secure Virtual Access is supported only on Windows clients.

Secure Virtual Access is similar to Secure Virtual Assist Unattended Mode in that administrator privileges are required to install these client features, and a technician is prompted to provide the password established during set-up to gain access to the system.

If Secure Virtual Access has been enabled on the Virtual Assist tab on the Portals > Portals page of the management interface, users should see a link on the Virtual Office portal to set-up a system for Secure Virtual Access. The following process allows Secure Virtual Access to be set-up on a system.

Step 1 Login to the Virtual Office portal through the system you wish to set up for Secure Virtual Access and click the **Virtual Access** link.

Step 2 A file should download with parameters to install the VASAC.exe file that will provide the needed client for Secure Virtual Access mode. Save and run the file.

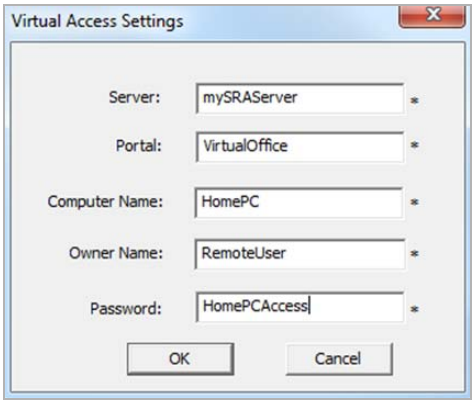

File Download - Security Warning
Do you want to run or save this file?
Name: ...g.sonicwall.com-443-admin-VirtualOffice-10.exe
Type: Application, 1.12MB
From: sslvpn.eng.sonicwall.com
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Note Running the file directly from this dialog box may not work on some systems. Save the file to the system and then run the application.

Step 3 Fill in the necessary information in the provided fields to set-up the system in Secure Virtual Access mode and click OK.

- **Server:** This should be the name or IP address of the appliance the technician normally accesses the Virtual Office from outside the management interface (Do not include “https://”).

- **Portal:** The name of the portal the technician would normally login to.
- **Computer Name:** This is an identifier for the system to help differentiate between other systems that may be waiting for support in the queue.
- **Password:** This is a password the technician must enter prior to accessing the system through the support queue.



Step 4 After installation, the VASAC client should be left running in the desktop tray.

This system's identifier name should now appear in the technician's support queue displayed on the **Secure Virtual Assist > Status** page within the management interface.Upon double-clicking the system listing, the technician will be prompted to provide the password established during system set-up to gain Secure Virtual Access to the system.

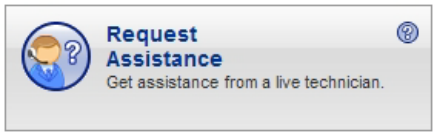
Ending Secure Virtual Access Mode

Disconnecting from a Secure Virtual Access session will place the system back in the support queue for later access by the technician. From the personal system-side, the user/technician may uninstall or terminate the application from the tray option icons.

An administrator can forcibly remove a system from the queue. If this occurs, the Secure Virtual Access system should no longer attempt to connect to the support queue and should display an error message.

Using the Request Assistance Feature

If the **Display Request Help Button** option has been enabled on the Virtual Assist tab on the Portals > Portals page of the management interface, users will see the **Request Assistance** button on the Virtual Office portal. By clicking this button on the portal, the user is placed in the Virtual Assist support queue for assistance.



For information on using Virtual Assist from the customer perspective, see "Initiating a Secure Virtual Assist Session from the Customer View" on page 90.

A technician who is currently assisting a user can also click this button to place the user back on the queue. Someone else in a technician role can then service this user by viewing the system and taking control of the user's mouse and keyboard. This is useful if one technician needs to hand the user off to another technician, because of differing areas of expertise or the end of shift.

Using Secure Virtual Meeting

Features

To set up a Virtual Meeting the meeting Coordinator performs the following steps:

- Log in
- Schedule a meeting
- Invite meeting attendees
- Optionally, create a poll for the invited attendees
- Start the meeting
- Use meeting features during a meeting
- End the meeting

The functions you are allowed to perform depend on your role and whether a meeting is in progress, as explained in “Coordinator Role” on page 105 and “Participant Role” on page 117.

User Roles

Secure Virtual Meeting has several user roles:

- **Coordinator** (Owner of the meeting) - The Coordinator must be a Dell SonicWALL SRA user on the appliance. The Coordinator schedules, sets up, and controls the meeting. In addition, the Coordinator has the sole power to promote a Participant to the Assistant.
- **Assistant** (Coordinator-designated Assistant) - The Coordinator selects an Assistant from the list of available Participants and assigns the Assistant privileges. When the Coordinator exits the meeting, the Assistant automatically becomes the Coordinator. A meeting may have multiple Assistants, each with the same or a different set of privileges. An Assistant need not be a user of the SSL-VPN appliance. Possible Assistant privileges are:
  - Start/End Meeting
  - Set Host
  - Open Polling
  - Set/Unset View Only
  - Invite Participants
  - Kick out Participants
  - Reschedule Meeting
- **Host** - The Host is a Participant who shares their desktop with all Participants in the meeting. When a meeting begins, the Host’s desktop is shown to all Participants. The Host can be changed by the Coordinator during the meeting by selecting any available Participant. If a Host is not explicitly set when the meeting starts, the Coordinator becomes the Host. Only one Participant is designated as the Host at any one time.

  Only the Host can control the Host System, unless the Host grants permission when a Participant requests control. The Host may also give control to any Participant by selecting the Participant from the Meeting Members list. Only one Participant can control the Host System at any one time. When a Participant takes control of the Host System, he loses control as soon as the Host moves his mouse pointer on the screen. The meeting control permission state is visible to all Participants while in the lobby.

- **Participant** (User with credentials to join the meeting) - A Participant must enter a meeting code before they can join a meeting. The code required to join the meeting is determined by the Coordinator prior to the meeting. After joining a meeting, the Participant can view the shared desktop and chat with another attendee privately or type a message in the Chat window that is visible to all attendees. A Participant becomes the Assistant if selected by the Coordinator or by an Assistant who has the required privilege.
- **View-only Participant** (User with limited meeting capabilities) - The Coordinator may designate any Participant as a View-only Participant. A View-only Participant cannot be assigned any privileges nor become an Assistant or Host.

Roles are switched before or during a meeting. A Coordinator or Assistant with necessary privileges can change the roles of any Participant during the meeting. A Participant wishing to become the Host must request permission from the Coordinator.

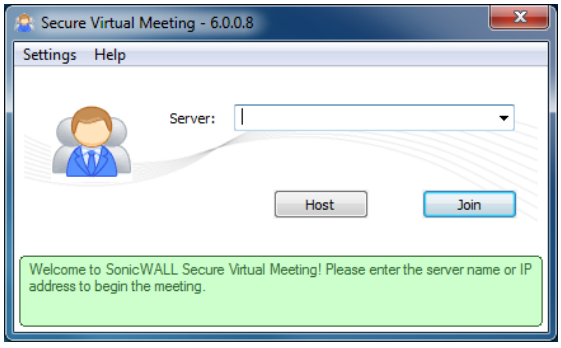
Coordinator Role

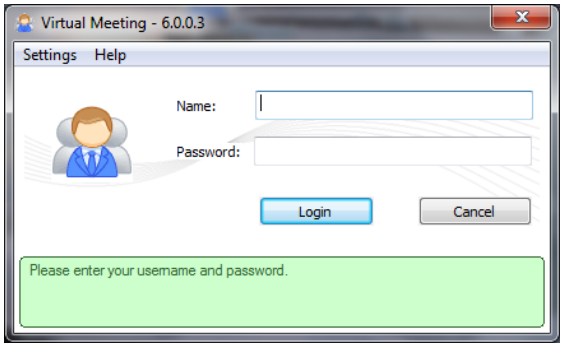
The Virtual Meeting Coordinator performs the following tasks:

Coordinator Tasks	Description
Logging In	Log in from a Virtual Meeting client using SRA credentials.
Setting Up a Meeting	Set up a meeting by scheduling a time and creating a meeting code that allows meeting members to join the meeting.
Performing Lobby Functions	Access various meeting functions in the lobby before or during a meeting.
Controlling Roles	Control what meeting members may do and appoint an Assistant to help facilitate the meeting.
Revising Meeting Settings	Set up a proxy or modify login profiles for meetings.
Logging Actions and Messages	Review a log of actions that occurred and view any warning or error message details that may require attention.
Starting a Meeting	Start a meeting immediately or at the scheduled time.
Using the Control Menu During a Meeting	Access functions available while a meeting is active.
Creating Email Invites	Invite meeting members through email before or during a meeting.
Polling	Create a poll for attendees to participate in.
Text Chatting	Chat with everyone or specific individuals in a meeting.

Logging In

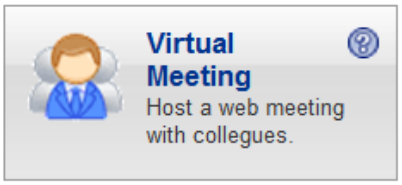
A Participant can join a Virtual Meeting by clicking a link in the email invite or by logging into the Virtual Meeting client if the Administrator has enabled Join Without an Invitation on the AMC **Secure Virtual Meeting > Settings** page. To login from an installed Virtual Meeting, click the **Host** button.


Secure Virtual Meeting - 6.0.0.8
Settings Help
Server:
Host
Join
Welcome to SonicWALL Secure Virtual Meeting! Please enter the server name or IP address to begin the meeting.

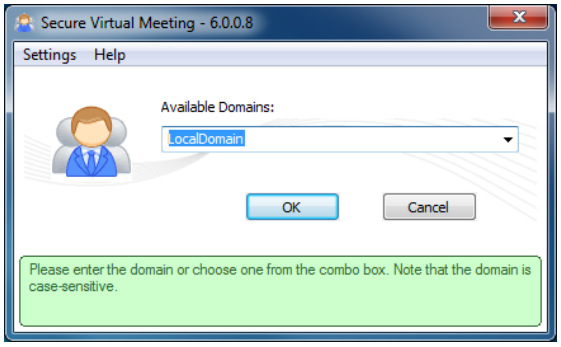


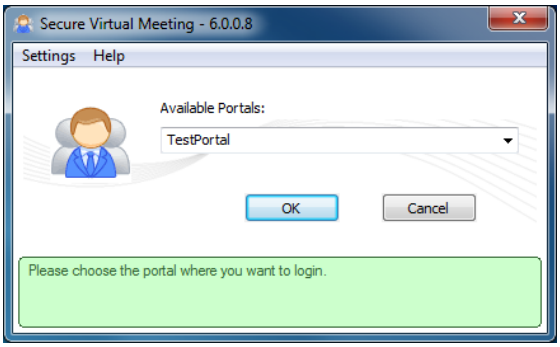
Only SRA users can be a Coordinator under normal circumstances, so SRA credentials are required for Coordinator login. However, a non-SRA user can become the Coordinator if the Participant is chosen as an Assistant and the Coordinator quits the meeting.

The meeting application can alternatively be accessed directly from the Virtual Office on an SRA 4200 and Virtual Appliance.



A **Domains** drop-down list is displayed if the user belongs to multiple domains, and a **Portals** drop-down list is shown if Virtual Meeting is enabled on multiple portals. Otherwise, the domain and portal is automatically selected.

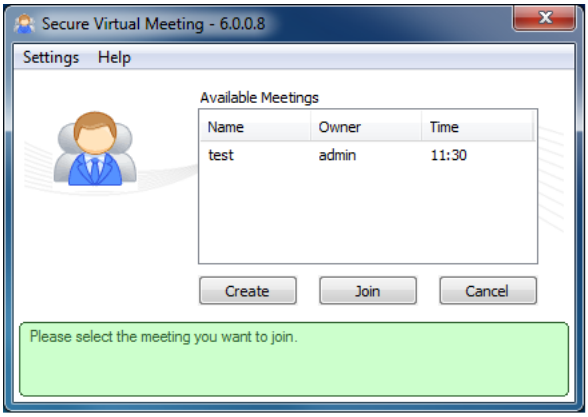

Secure Virtual Meeting - 6.0.0.8
Settings Help
Available Domains:
LocalDomain
OK
Cancel
Please enter the domain or choose one from the combo box. Note that the domain is case-sensitive.

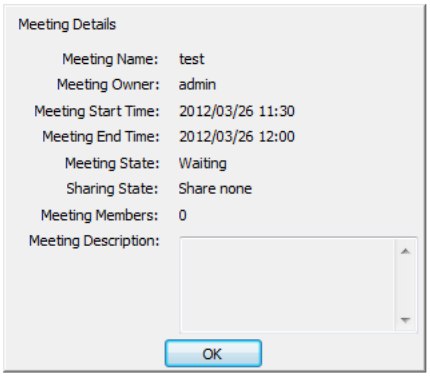


Select the desired portal to be used for the meeting. Only Participants who are in the selected portal will be able to join the meeting.

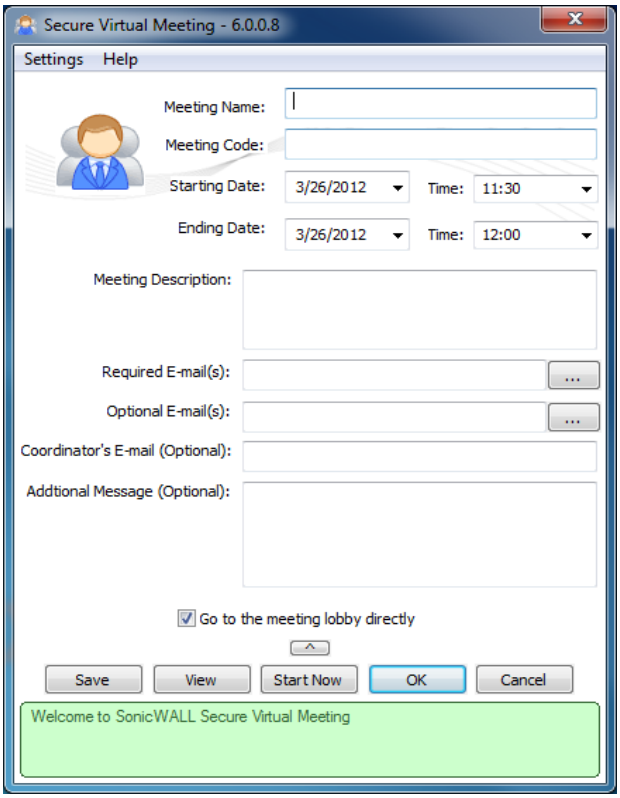
Setting up a Meeting

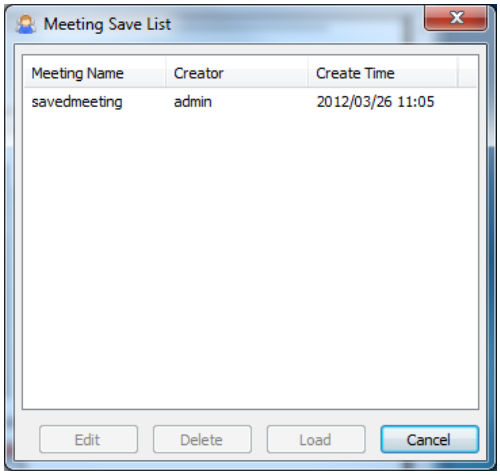
Once logged into the system, the option to create a meeting is available. If a meeting is already created you may view the details of the meeting by right-clicking the desired meeting and selecting **Properties**.





To create a meeting, click the **Create** button to display the meeting creation interface.



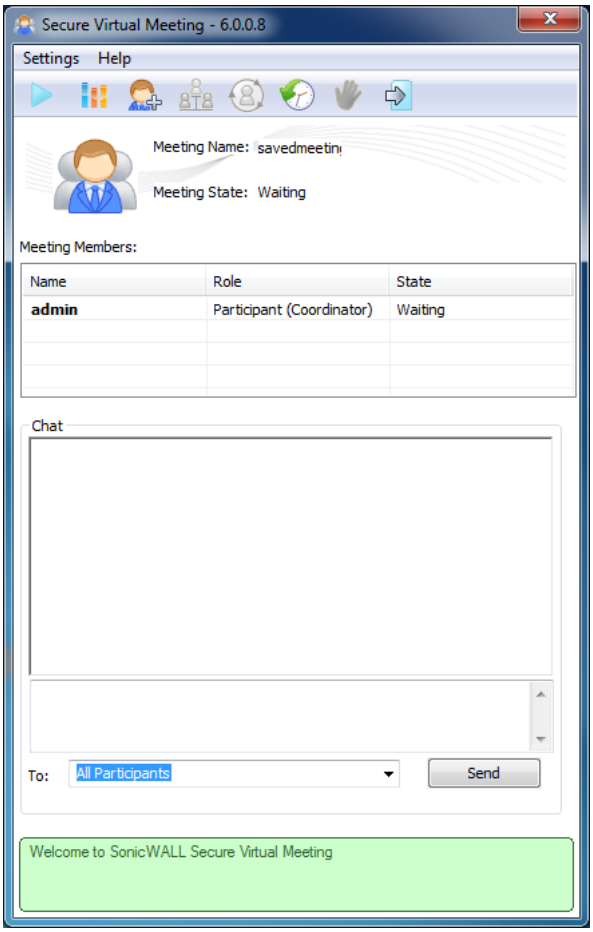


To set up a meeting enter a **Meeting Name**, **Meeting Code**, **Starting Date** and **Time**, and **Ending Date** and **Time**. The meeting code will be entered by all Participants wishing to join the meeting. If you want to invite attendees and the Email fields are not visible, click the down arrow button directly below the **Ending Date** field. You can then identify who should receive meeting email invitations.

Use the buttons across the bottom of the window to perform the following functions:

Save	Saves the meeting for future editing.
View	Displays previously saved meetings.
Start Now	Starts the meeting immediately with the current user system time, and enter the lobby.
OK	Start the meeting immediately at the next available time slot (based on the current time), and enter the lobby.

After you create a meeting, you enter the meeting's lobby automatically.



When a meeting is scheduled for a later time, the Coordinator exits the meeting and returns to the lobby at the meeting start time. If the **Allow starting meeting without meeting creator** setting is disabled and the Coordinator has not joined the meeting by the start time, the participants will be kept waiting in the lobby until the scheduled meeting end time (when all participants automatically exit the lobby). If the **Allow starting meeting without meeting creator** setting is enabled and the Coordinator has not joined the meeting by the start time, within two minutes past the scheduled start time, an existing participant is chosen randomly to become the Coordinator.

If the Coordinator enters but does not start the meeting, when the meeting time ends the Coordinator receives a notification to reschedule or end the meeting. When the end time is reached, the meeting ends and all meeting members automatically exit the meeting.

In the lobby you can manage the meeting, set roles, and many other functions described in “Performing Lobby Functions” on page 109, depending on your role.

Performing Lobby Functions

The following functions can be performed from the lobby by clicking buttons:

Clicking the **Start Meeting** button starts the meeting. Only the Coordinator and Assistant can start a meeting.

Clicking the **Stop Meeting** button stops the meeting. Only the Coordinator and Assistant can end the meeting.

Clicking the **Polling** button opens the polling window where you can load, edit, and start a poll for Participants currently in the meeting. Only the Coordinator and Assistant can initiate polling. Polling details are described in“Polling” on page 115.

Clicking the **Invite** button sends an email invitation to Participants. Only the Coordinator and Assistant can invite Participants. Invite details are described in “Creating Email Invites” on page 113.

Clicking the **Reschedule Meeting** button reschedules the meeting start and end times. Only the Coordinator and Assistant can reschedule a meeting.

Clicking the **Request Host** button informs the Host that you want to become the Host and share your desktop. Only Participants who are not currently the Host can request to become the Host.

Clicking the **Quit** button exits the meeting and return to the meeting selection window. Anyone in the meeting can quit the meeting.

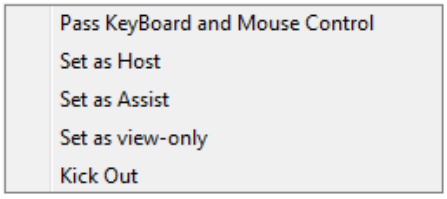
Clicking the **Start Sharing** button shares the Host desktop with all Participants in the meeting. Sharing is only available during a meeting.

Clicking the **Stop Sharing** button stops sharing the Host System desktop. Only the Host can stop sharing and only while in the sharing state (after Start Sharing has been selected).

Clicking the **Request Control** button requests that the Host give you control of the keyboard and mouse. Only Participants who aren’t the Host can request control.

Controlling Roles

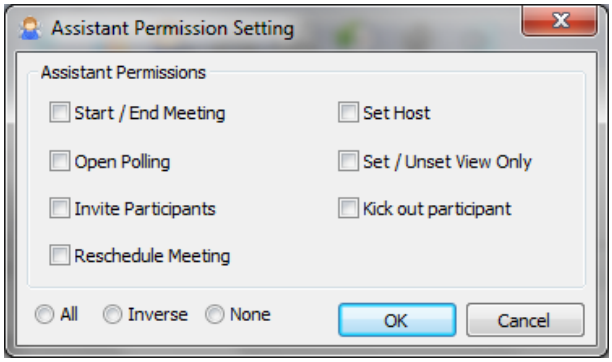
The Coordinator and Assistant can change a meeting member’s role by right clicking the meeting member’s name and selecting a role from the drop-down menu.



The following options may appear, depending on permissions and the meeting member's current role.

Option	User	Description
Pass Keyboard and Mouse Control	Host	Allow the selected Participant to control the Host's PC.
Set as Host	Coordinator Assistants with Set Host permission	Set the selected Participant to be the Host.
Set as Assistant	Coordinator	Set the selected Participant to be the Assistant. An Assistant has privileges similar to the Coordinator, depending on the settings selected by the Coordinator as shown below.
Set as view-only	Coordinator Assistant	Set the selected Participant to view-only mode so the Participant can only view the Host desktop (cannot request control).
Kick out	Coordinator Assistant	Remove the selected Participant from the meeting.

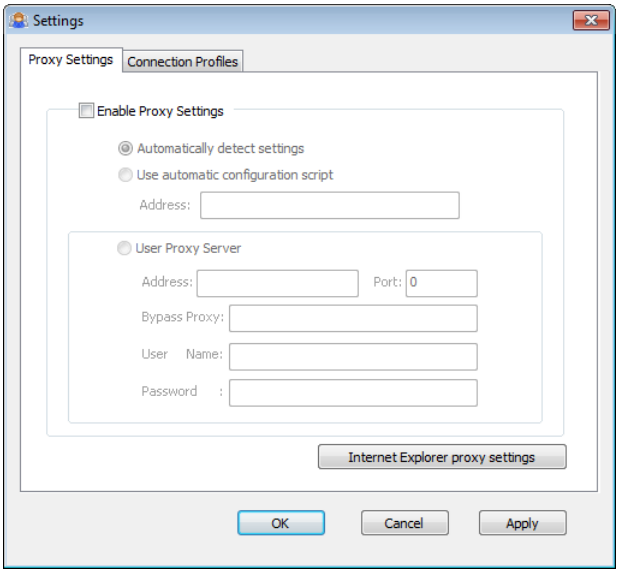
.



Revising Meeting Settings

Proxy Settings

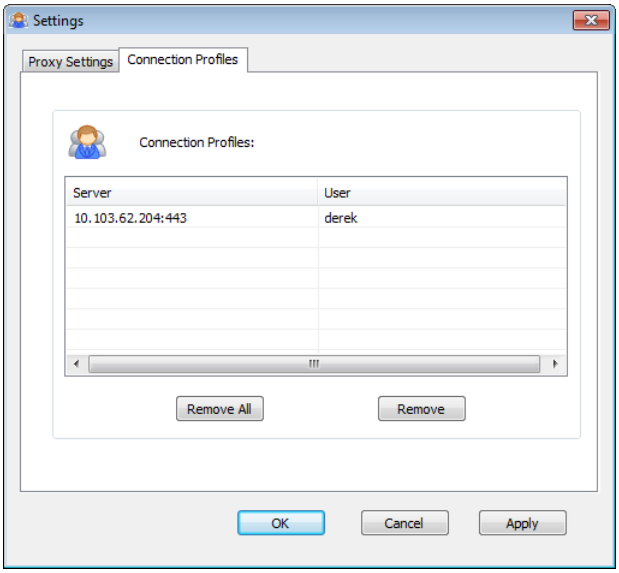
For setups that require a proxy, click the **Settings** tab in the Virtual Meeting window, and check the **Enable Proxy Settings** check box.



Enter the proper information to utilize the proxy or click the **Internet Explorer proxy settings** button to automatically import the proxy settings used by Internet Explorer.

Connection Profiles

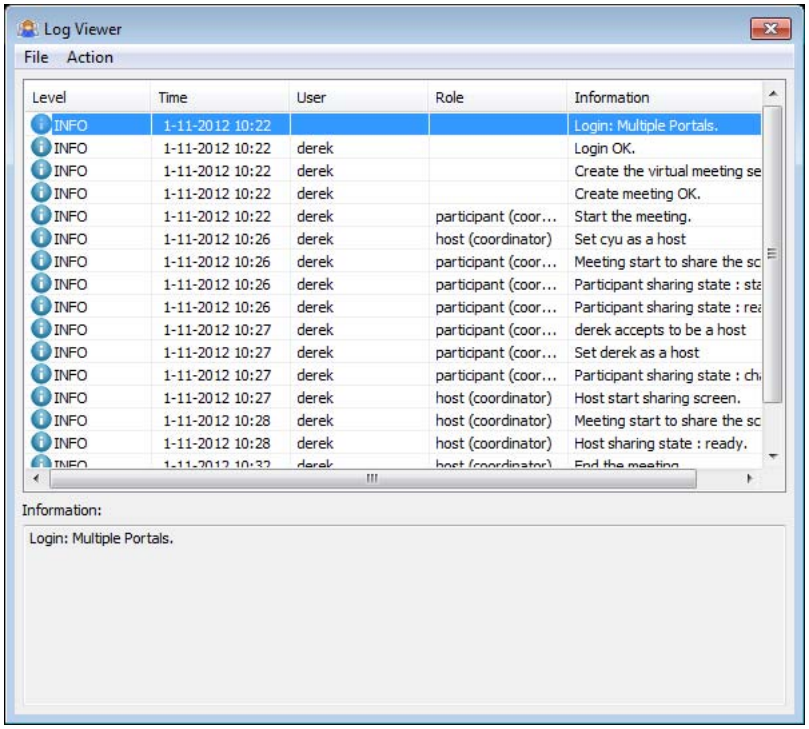
For users accessing different appliances, profiles are shown on the Connection Profiles window. Information about the server currently in use is automatically populated for convenience.



To remove all connection profiles, click the **Remove All** button. To remove a specific connection profile, select the connection profile and click the **Remove** button.

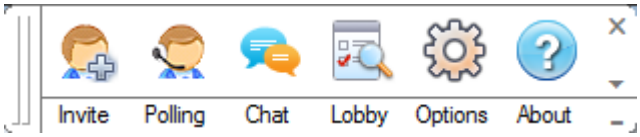
Logging Actions and Messages

The Log Viewer displays all event log data, which includes actions taken during a meeting and any errors that occur. The Log helps you keep track of events that occur in a meeting and shows all actions performed by meeting Participants. Use the error and warning events in the log to take the appropriate corrective action, if necessary.


Log Viewer
File Action
Level Time User Role Information
INFO 1-11-2012 10:22 Login: Multiple Portals.
INFO 1-11-2012 10:22 derek Login OK.
INFO 1-11-2012 10:22 derek Create the virtual meeting se
INFO 1-11-2012 10:22 derek Create meeting OK.
INFO 1-11-2012 10:22 derek participant (coor... Start the meeting.
INFO 1-11-2012 10:26 derek host (coordinator) Set cyu as a host
INFO 1-11-2012 10:26 derek participant (coor... Meeting start to share the sc
INFO 1-11-2012 10:26 derek participant (coor... Participant sharing state : sta
INFO 1-11-2012 10:26 derek participant (coor... Participant sharing state : rea
INFO 1-11-2012 10:27 derek participant (coor... derek accepts to be a host
INFO 1-11-2012 10:27 derek participant (coor... Set derek as a host
INFO 1-11-2012 10:27 derek participant (coor... Participant sharing state : cha
INFO 1-11-2012 10:27 derek host (coordinator) Host start sharing screen.
INFO 1-11-2012 10:28 derek host (coordinator) Meeting start to share the sc
INFO 1-11-2012 10:28 derek host (coordinator) Host sharing state : ready.
Information:
Login: Multiple Portals.

Using the Control Menu during a Meeting

The Control Menu is available at the top of a shared desktop when the Host shares the desktop during an active meeting.



The **Invite** button is available for the Coordinator or Assistants with invite permission. It opens the invite dialog if the lobby is not open. Invite details are described in "Creating Email Invites" on page 113.

The **Polling** button is available for the Coordinator or Assistants with polling permission. It opens the polling dialog detailed in "Polling" on page 115.

The **Chat** button is available for all Participants, including View-only Participants. It opens a chat dialog if the lobby is not open. Chat details are described in "Text Chatting" on page 117.

The **Lobby** button is available for all meeting members, including View-only Participants. If the lobby is hidden during a meeting, it displays the lobby window when the Host is sharing the screen.

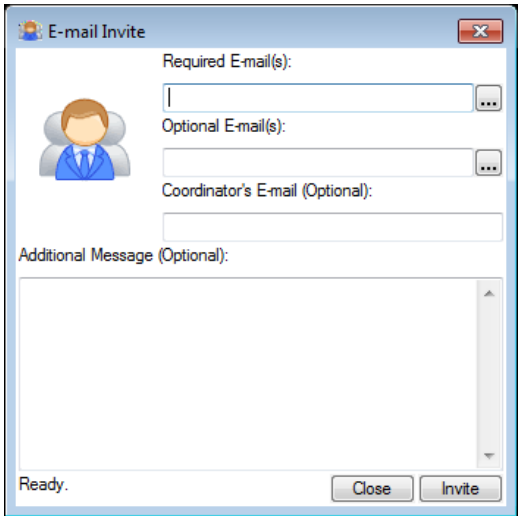
The **Options** button opens the Meeting Settings window described in *"Revising Meeting Settings" on page 111* and is available for all Participants.

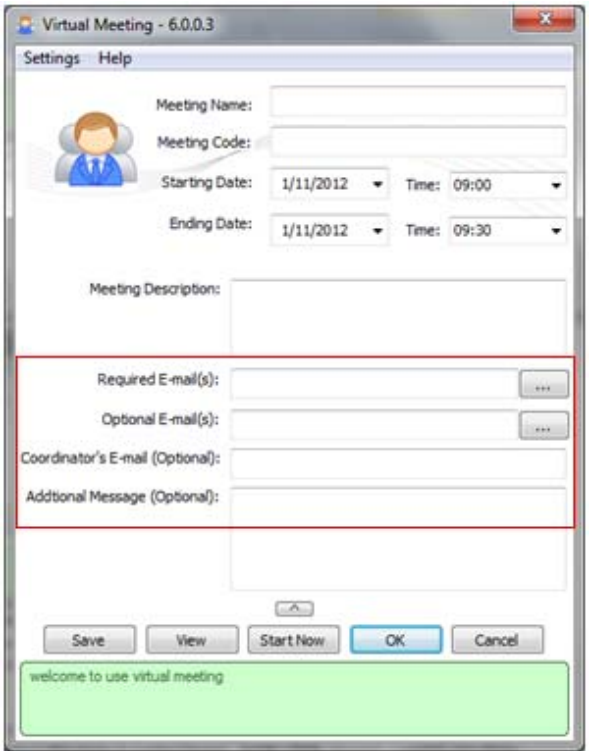
The **Viewer** button is available for all Participants except the Host. It toggles the window between the Participant's window and the Host's desktop.

The **About** button opens the About dialog, which identifies the Secure Virtual Meeting client and version. The **About** button is available for all meeting members, including View-only Participants.

Creating Email Invites

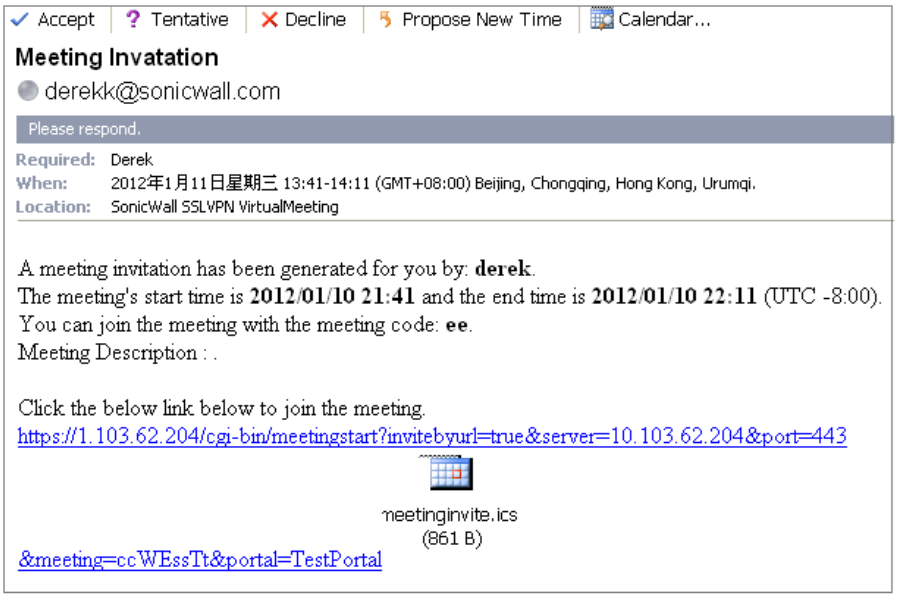
Invitations can be sent when creating the meeting or while in an active meeting.





Note Email settings must be configured in the management console **Log > Settings** page before Virtual Meeting email can be sent.

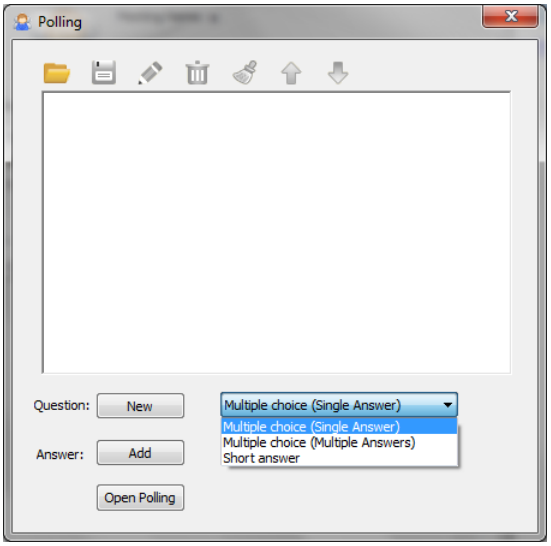
To invite someone to a Virtual Meeting, enter the email address and click **Invite**. Additional fields are optional. Invited users receive an email similar to the following:


Accept
Tentative
Decline
Propose New Time
Calendar...
Meeting Invatation
derekk@sonicwall.com
Please respond.
Required: Derek
When: 2012年1月11日星期三 13:41-14:11 (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi.
Location: SonicWall SSLVPN VirtualMeeting
A meeting invitation has been generated for you by: derek.
The meeting's start time is 2012/01/10 21:41 and the end time is 2012/01/10 22:11 (UTC -8:00).
You can join the meeting with the meeting code: ee.
Meeting Description : .
Click the below link below to join the meeting.
https://1.103.62.204/cgi-bin/meetingstart?invitebyurl=true&server=10.103.62.204&port=443
meetinginvite.ics
(861 B)
&meeting=ccWEssTt&portal=TestPortal

After receiving the email invitation, attendees click the link in the email, which accesses the appliance to join the meeting. If the Secure Virtual Meeting plug-in is installed, it automatically downloads and launches the application and puts the attendee into the meeting. Alternatively, attendees can manually download the Secure Virtual Meeting plug-in and run it as an application. Both cases will provide meeting access.

Polling

Click the Open Polling button to display the Polling window where you can create polls and define the polling questions.



Create new questions by clicking the and buttons. There are three question types:

- Multiple choice (single answer)
- Multiple choice (multiple answer)
- Short answer

Use the buttons at the top of the window to:

The **Open Virtual Meeting Poll Files** button opens any saved polling questions and possible answers.

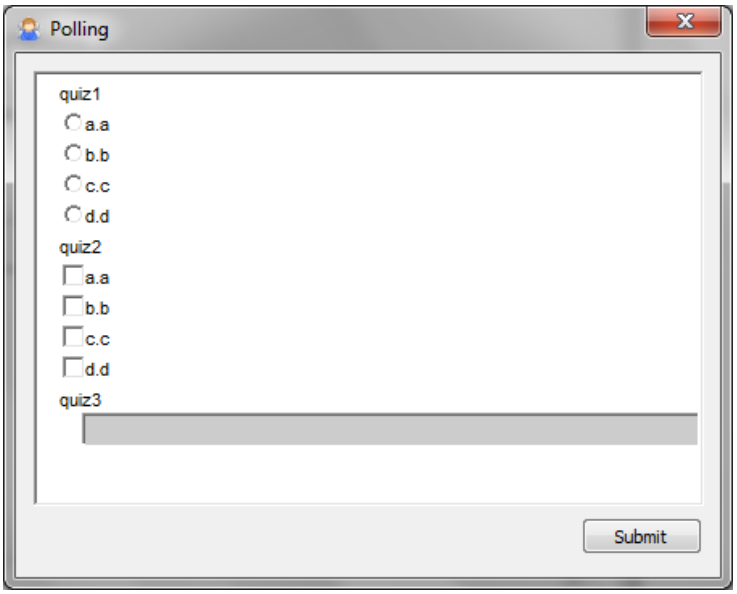
The **Save Virtual Meeting Poll File** button saves the current polling questions and answers.

The **Edit** button is used to edit the currently selected polling question or answer.

The **Clear** button erases ALL polling questions and answers.

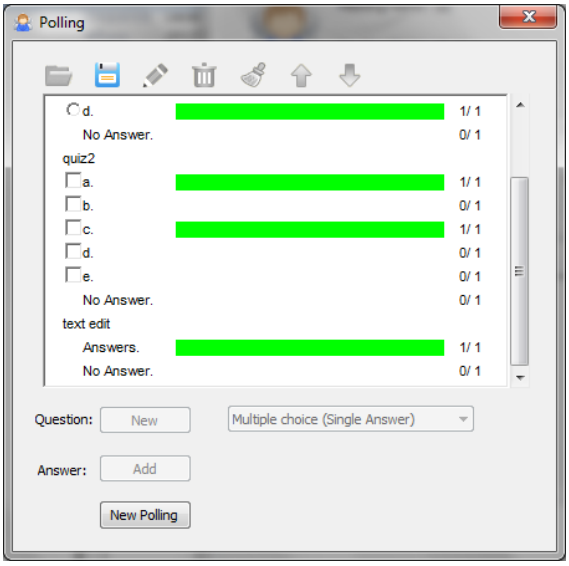
The **Up** and **Down** buttons change the order of the selected questions or possible answers.

Click the Open Polling button to start polling and send the poll to the selected Participants to answer.



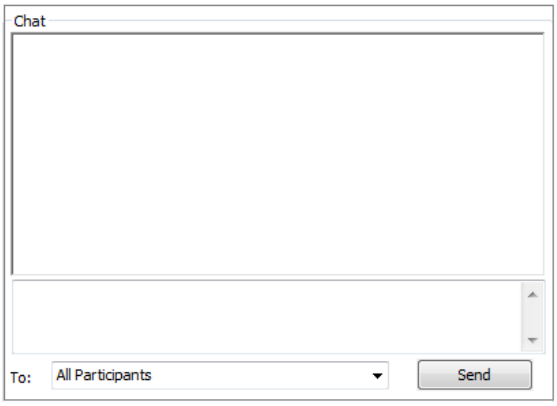
Polling feedback window

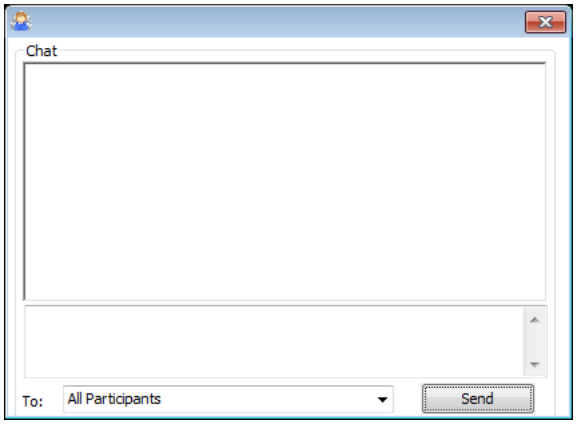
Feedback from the poll is returned to the poll initiator when answers are submitted and when the **End Polling** button is clicked. The collected feedback is displayed as shown below. Click the green bar to display detailed information for each answer.



Text Chatting

Chat with all attendees in the meeting or have a private chat with one or more selected attendees, including View-only Participants.





If the lobby is hidden, click on the control menu once the meeting has started and the Host is sharing the screen. The chat window is displayed in a stand-alone chat window.

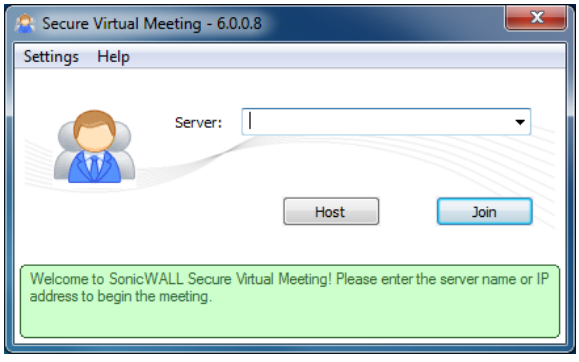
Participant Role

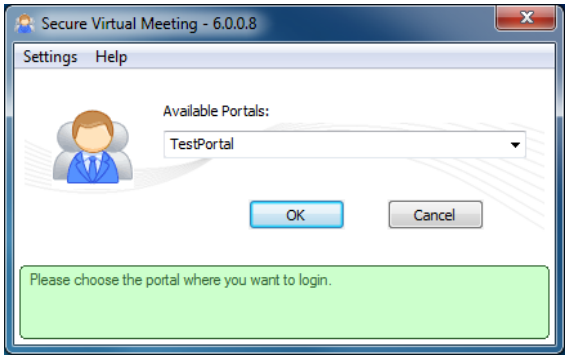
Participants can be designated as View-only Participants or regular Participants. View-only Participants enter and exit meetings like other Participants, but cannot perform most functions. However, they can be kicked out of meetings like other regular Participants. Regular Participants can also:

- Respond to polls
- Text chat
- Request control of the Host keyboard and mouse
- Request to become the Host and share the Participant's desktop
- Become the Assistant
- Become a View-only Assistant

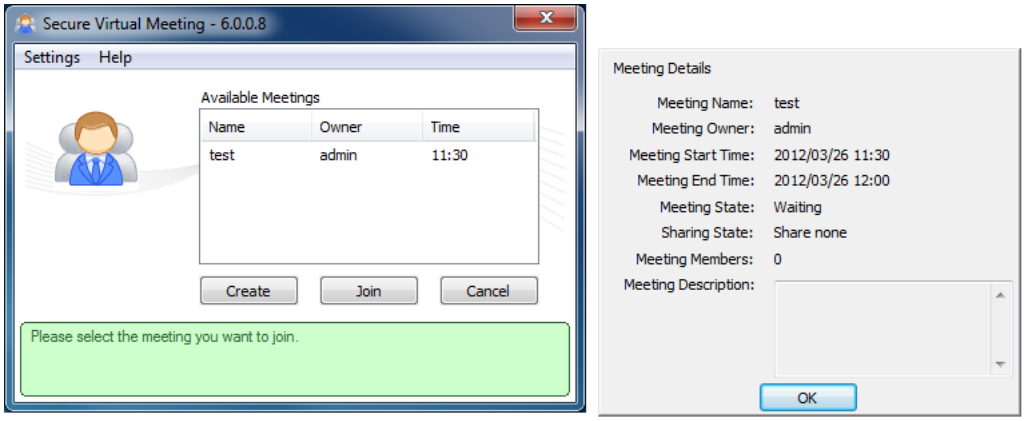
Login

Participants click the link from the meeting email invitation or type the server name or IP address in the **Server** field of the Secure Virtual Meeting window.

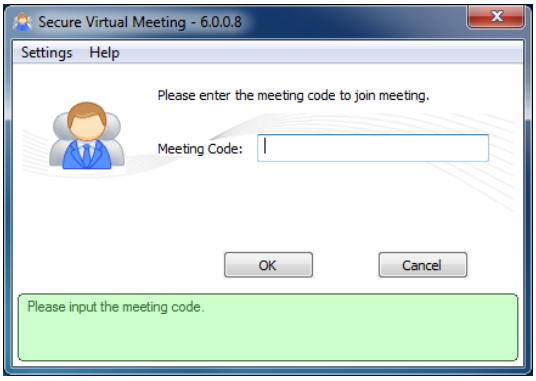

Secure Virtual Meeting - 6.0.0.8
Settings
Help
Server:
Host
Join
Welcome to SonicWALL Secure Virtual Meeting! Please enter the server name or IP address to begin the meeting.



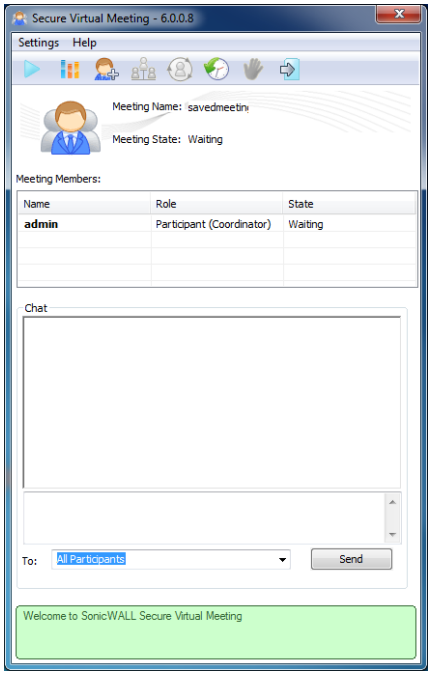
If necessary, select the proper meeting portal. All available meetings are displayed.



Select the meeting to join and click the **Join** button. The following prompt is displayed if you are required to enter a meeting code to join the meeting.


Secure Virtual Meeting - 6.0.0.8
Settings Help
Please enter the meeting code to join meeting.
Meeting Code:
OK Cancel
Please input the meeting code.

Enter the meeting code that was provided in the meeting email invitation and click the **OK** button to join the meeting. After joining the meeting, you will be in the meeting lobby.



Using File Shares

File shares provide remote users with a secure Java applet or HTML-based interface to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.

The File Shares Applet mimics Windows Explorer navigation and provides functionality not available in HTML-based File Shares, including the ability to overwrite existing files and upload directories.

This section contains the following subsections:

- "Using the File Shares Applet" section on page 119
- "Using HTML-Based File Shares" section on page 130

Using the File Shares Applet

The File Shares Applet has a similar look and feel to the Windows Explorer tool, featuring drag-and-drop and multiple file selection capabilities. It also provides the user the ability to set up bookmarks to quickly navigate through networks from the portal level. This feature saves time lost moving through network and server paths. The File Shares Applet leverages Sun's Java platform browser plug-in to increase usability by mimicking the common Windows Explorer interface. With the help of the HTTPS protocol, the applet securely transfers encrypted files and information to and from the SRA appliance. The appliance communicates this data to the individual machines on the remote network.

This section contains the following subsections:

- "User Prerequisites" section on page 119
- "Configuration Overview" section on page 119
- "Configuration Examples" section on page 124

User Prerequisites

The Dell SonicWALL SSL VPN File Shares Applet is a Java application that supports Java 1.3.1 and newer, and the JRE Version 5.0 Update 10 or newer is recommended. To download the latest Java and JRE versions, visit http://www.java.com. Internet Explorer 6.0, Firefox 1.5 or newer, Opera 8 or newer, and Safari RSS are recommended Web browsers of optimal performance of the Java File Shares feature.

The administrator must enable the File Shares Applet for users to use it.

There must be a computer with open access for the Dell SonicWALL SSL VPN File Shares Applet to log into. The remote computer must have shared folders for files to be copied or moved. Sharing policy must be set from within the remote computer's own operating system.

Configuration Overview

The SSL VPN File Shares Applet is easy and intuitive to use. User should be aware of its functions and limitations. Setting up bookmarks and the browser interface are covered in this section, along with an overview of the browser and sample use cases.

This section contains the following subsections:

- "Setting up Bookmarks" section on page 120
- "Using the Java File Shares Applet" section on page 121
- "File Shares Applet Browser Overview" section on page 123

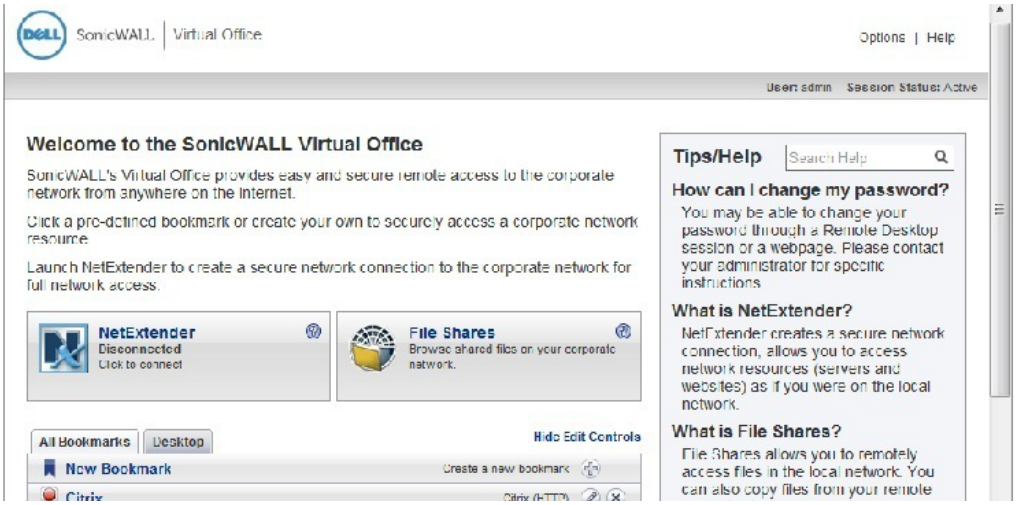
Setting up Bookmarks

Bookmarks can be set up for folders and for files. A file bookmark will not launch the Applet, but instead will download and launch the file directly. Bookmarks must be enabled by the administrator. To set up bookmarks from the Virtual Office Portal, perform the following steps.

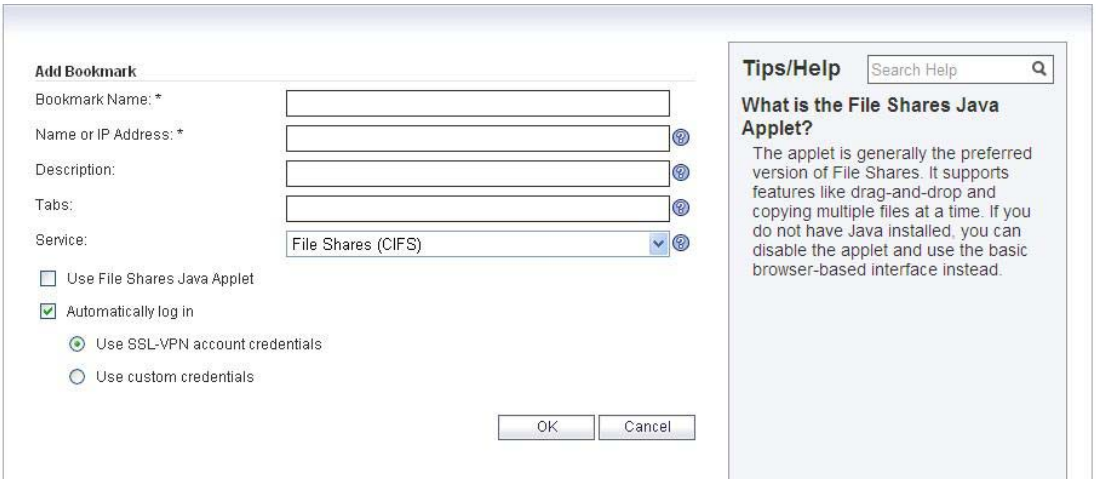
Step 1 Open a Web browser and log into the SSL VPN Virtual Office interface by typing the URL in the **Location** or **Address** bar and press **Enter**. Type in your user name in the **User Name** field and your password in the **Password** field, then select the appropriate domain from the **Domain** drop-down. Click **Login**.

Step 2 Click the **Show Edit Controls** link in the middle of the portal page.

Step 3 Click the **New Bookmark** tab in the portal page.



Step 4 The Add Bookmark screen displays. Enter a friendly name for the bookmark in the **Bookmark Name** field.


Add Bookmark
Bookmark Name: *
Name or IP Address: *
Description:
Tabs:
Service:
File Shares (CIFS)
Use File Shares Java Applet
Automatically log in
Use SSL-VPN account credentials
Use custom credentials
OK
Cancel
Tips/Help
Search Help
What is the File Shares Java Applet?
The applet is generally the preferred version of File Shares. It supports features like drag-and-drop and copying multiple files at a time. If you do not have Java installed, you can disable the applet and use the basic browser-based interface instead.

Step 5 Enter the IP address and file directory path to the File Share in the **Name or IP Address** field.

Note When using the Java applet, the **Name or IP Address** field must be to a file directory and end with a / or \ character.

Step 6 In the **Service** pull down menu, select the **File Shares (CIFS)** option.

Step 7 Check the **Use File Shares Java Applet** box to enable the File Shares Applet for this bookmark. Leaving this box unchecked means the portal will launch the original HTML browser when the bookmark is selected.

Step 8 Optionally, select **Automatically log in** to log in to this file share using either your SSL VPN credentials or by specifying custom credentials.

Step 9 Click **Add**.

Bookmark serve as useful shortcuts to quickly access different network locations. Bookmarks can also be set up from the File Shares Browser, either by clicking the **Bookmark** button, or using the bookmark option from the right-click menu.

Using the Java File Shares Applet

While loading the browser interface, warning messages might display. These messages will look different for different browsers. For the purpose of these examples, Internet Explorer 6.0 was used.

Step 1 If you are not logged into the SSL VPN Virtual Office user interface, open a Web browser and type the Virtual Office interface URL in the **Location** or **Address** bar and press **Enter**. Type in your user name in the **User Name** field and your password in the **Password** field, then select the appropriate domain from the **Domain** drop-down menu. Click **Login**.

Step 2 Launch File Shares Applet by clicking the **File Shares** button, or clicking on a link with the File Shares Applet enabled. The File Shares Applet will launch in a new window, separate from the Virtual Office portal.

Step 3 Depending on available browser and Java plug-in, a warning may display, click **OK** to continue.

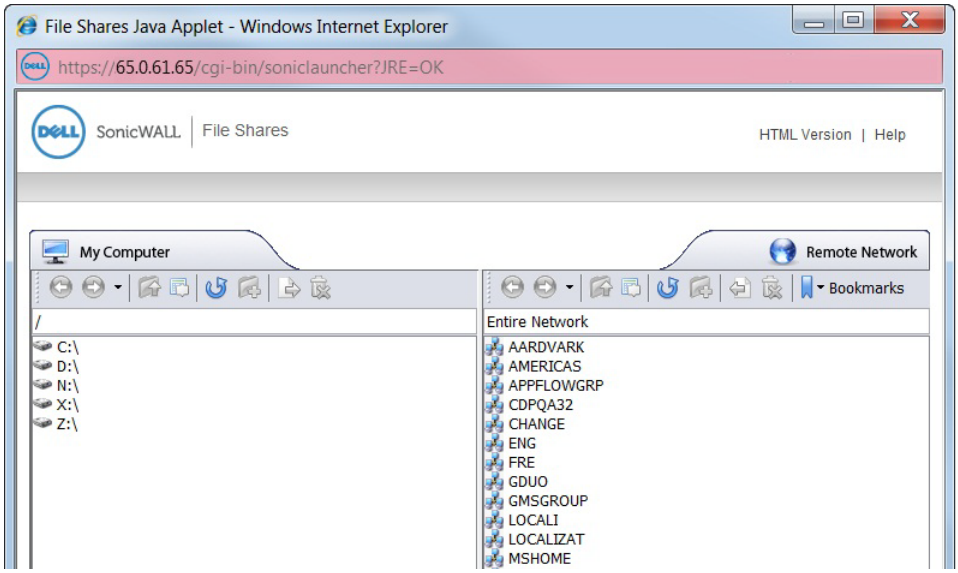
Windows Internet Explorer
Warning, you may not be running the optimal browser and Java Version for this product. Some features may not be available while running the File Shares Java Applet from this machine. Click OK to continue.
OK
Cancel

Note To avoid this warning, upgrade browser to Internet Explorer 8.0 or newer, Firefox 16.0 or newer, Chrome 22.0 or newer, or Safari 5.0 or newer. Also updates to Java 5.0 Update 10 or newer are recommended.

Step 4 Depending on the networks configurations and browser, one or more security warnings may display. Follow the instructions to accept the certificate for the server.

This Connection is Untrusted
You have asked Firefox to connect securely to sslvpn.sonicwall.com, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

The File Shares Applet displays.



Note The File Shares Applet window will not automatically refresh when its contents have changed or if it has been previously viewed. To refresh, click the **Refresh** icon from the toolbar, or use the **Refresh** option from the right-click menu.

Note The remote network can be browsed from the remote window's address bar. The local directory can not be changed from the address bar. The remote path is capped at 1024 characters. The actual maximum string size will change depending on language.

Step 5 To select multiple items, click the items while holding the **shift** or the **ctrl** key. Clicking on an item again will de-select it and remove it from the group.

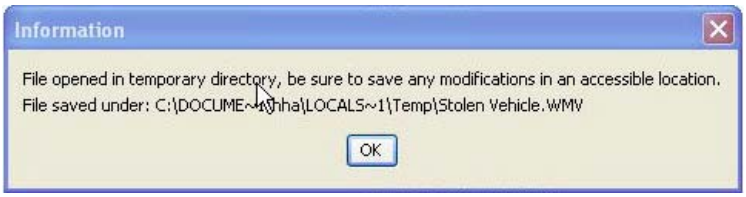
Step 6 To copy a file or group of files either to or from the network, select desired items and **click-and-drag** them across the center boundary. This will copy the file(s) into the open directory. Alternatively, the file(s) can be copied directly into a folder by dragging the icon and dropping

over the desired folder; one could also use the **copy** button on the toolbar, or use the copy option from the right-click menu. A progress bar displays the waiting time required to copy the files.

Note The File Shares Applet supports overwriting existing files. If a file exists with the same name as the one you are trying to copy over, the Applet will prompt you to rename the file being copied. If the name is kept the same, the copied file will overwrite the existing one.

Step 7 **Double click** on a file to launch it with the proper application. If activating a file on the remote machine, the File Shares Applet will first download the file to a temporary folder on your machine and then open it.

The File Shares Applet will not always be able to delete the temporary file after use. Use caution when opening files with sensitive material.


Information
File opened in temporary directory, be sure to save any modifications in an accessible location.
File saved under: C:\DOCUME~1\hha\LOCALS~1\Temp\Stolen Vehicle.WMV
OK

File Shares Applet Browser Overview

Each window, local and remote, contains a set of buttons for commonly used operations in the toolbar. Hovering the mouse cursor over these icons displays convenient tool tips to the user. Dragging the toolbar by the dotted line on the left side of it undocks the toolbar into its own window. To re-dock the toolbar, close the window. These are the same functions as those in the right-click menu.

Here is a list of the buttons on the task bar and their respective function.

- **Back**: Traverses back in the history. Sets the current view of the window to the previous location in history. This icon is dimmed if there is no previous history location.
- **Forward**: Traverses forward in history. This icon is dimmed if there are no forward locations in history.
- **Up**: Traverses up the directory tree to the parent directory of the current view. This icon is dimmed if the current view is of the root directory or if the parent directory cannot be resolved.
- **Refresh**: Refreshes the current view by either polling the local file system or remote network via the SSL VPN. The refresh icon will be dimmed in the remote window if its contents are currently being refreshed.
- **New Folder**: Creates a new folder within the respective file system. Clicking this icon displays the “New Folder” dialog box, allowing the user to assign a name to the new folder. This icon is dimmed when the location of the window is such that a new folder cannot be created. (for example, Root of a Windows filesystem, domain list, machine list).

- **Copy**: Copies the selected file(s)/folder(s) to the location of the remote window. Clicking this icon displays the “Copy” dialog box that will show the status information of the copy procedure. If the file being copied already exists, a new dialog will display asking the user whether or not the existing file should be replaced. The copy icon is dimmed when there are no selected files/folders to copy (for example, if no drive or domain is selected). It is also dimmed if the remote location cannot accept files copied to it (for example, Domain List/ Machine List). Copying a folder also copies everything within the folder.
- **Delete**: Deletes the selected file(s)/folder(s). Deleting a folder will delete everything within the folder.

Note Files deleted this way are fully removed from the original machine they were on. These files are not sent to the recycling bin and are in no way recoverable.

Configuration Examples

The following configuration examples provide a demonstration of the usefulness and flexibility of the File Shares Applet.

- Configuring Bookmarks from Within the File Shares Applet, page 124
- Using Bookmarks from Within the File Shares Applet, page 126
- Moving Files and Folders, page 127
- Launching a File Directly from the File Shares Applet, page 128

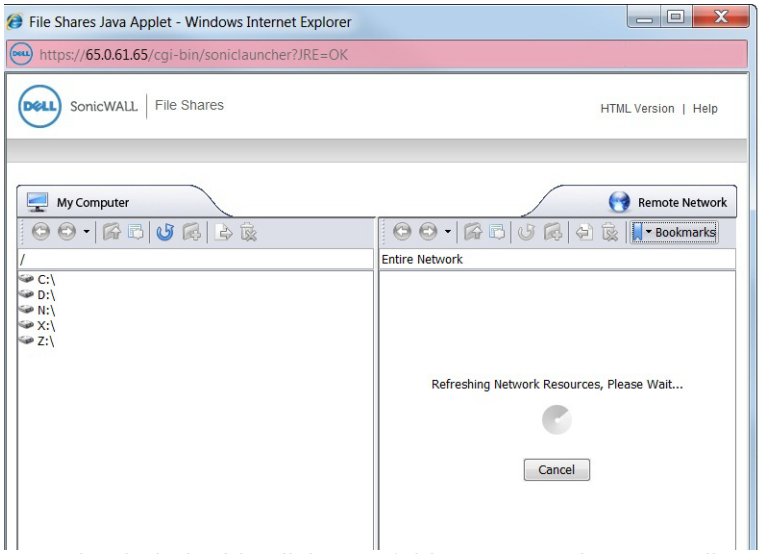
Configuring Bookmarks from Within the File Shares Applet

Navigating a remote computer’s directory hierarchy structure takes a long time. To reduce this process as much as possible, the Dell SonicWALL SSL VPN File Shares Applet allows the user to create bookmarks on the fly from within the File Shares Applet itself. This allows the user to skip the hierarchy structure of the remote computer the next time she needs to access a particular file or folder.

Step 1 Launch the File Shares Applet by clicking on the **File Shares** button in the Virtual Office portal. The File Shares Applet displays.

Step 2 The File Shares Applet's default location for the local window is the base directory, while the remote window shows the entire network. Double click on the appropriate folders to navigate the local window to the desktop or another appropriate folder.

Step 3 To navigate the remote window, double click on a visible computer, or input the name in the address bar preceded by **** and followed by a **** and press **Enter.** The File Shares Applet will then navigate to the requested computer. It may take several seconds for the resources to load, depending on the network configuration.

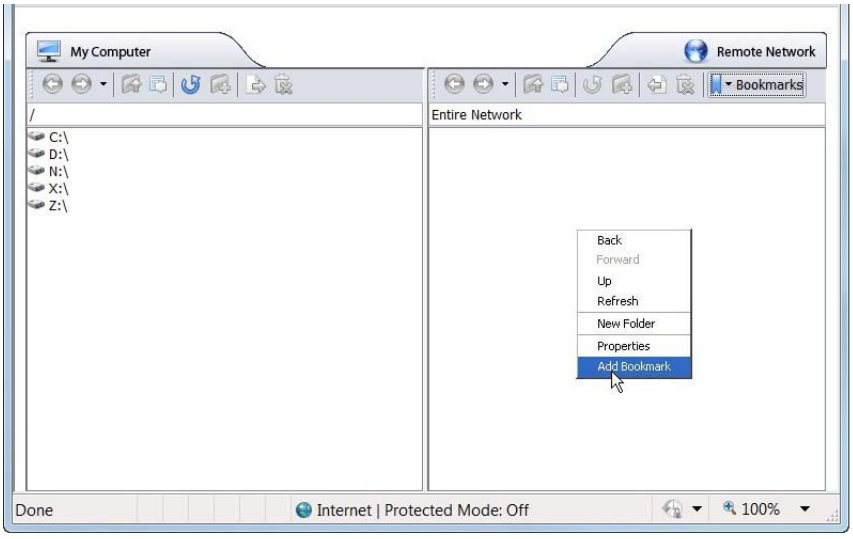


Step 4 Once loaded, double click on a folder or enter the target directory path within the address bar. This can take some time as the File Shares Applet must browse through the network after every change.

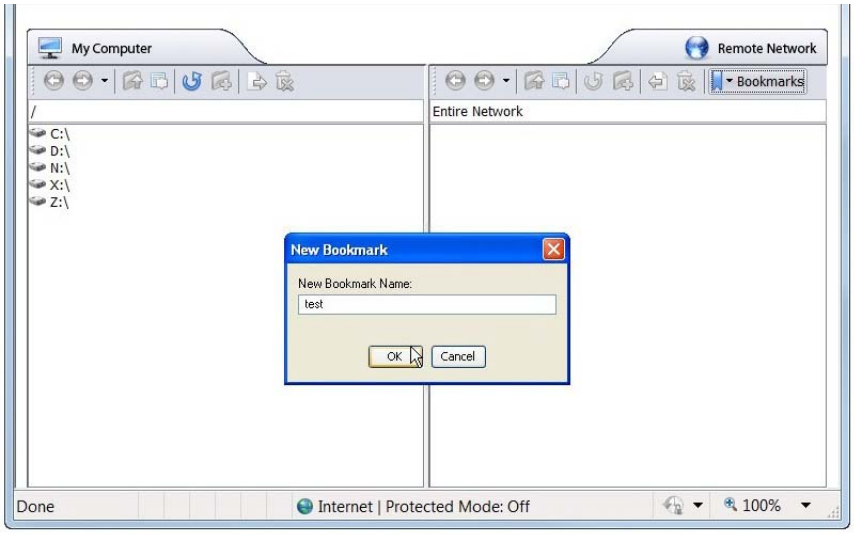
Note Only the remote window can use the address bar to navigate through a computer's file hierarchy.

Step 5 To set a bookmark to the current directory, right-click in an empty location in the remote directory and select **Add Bookmark**.

Note To set a bookmark for a specific file or folder, select it prior to selecting **Add Bookmark** from the right-click menu.



Step 6 Enter a name for the new bookmark in the New Bookmark window that displays.



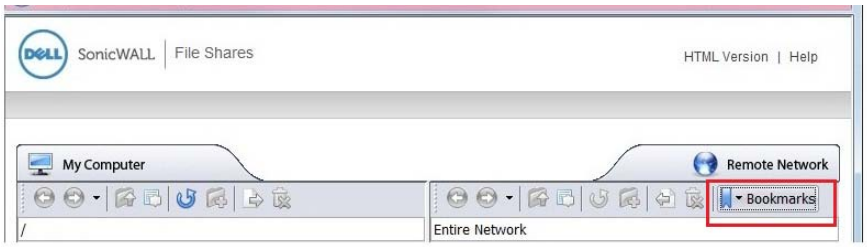
Step 7 Click **OK**. The bookmark is added to the Virtual Office portal. Clicking on the bookmark accesses the selected folder or file.

Using Bookmarks from Within the File Shares Applet

In Addition to accessing bookmarks from the Virtual Office portal, bookmarks can be easily accessed from within the File Shares Applet.

Step 1 Launch the File Shares Applet by clicking on the **File Shares** button in the Virtual Office portal.

Step 2 Click on the **Bookmarks** button on the task bar in the remote window. A pull down menu displays with the message **Loading Bookmarks**. Keep the mouse within the pull down menu as the File Shares Applet loads the bookmarks.



Step 3 Once loaded, click book mark to load the desired file or folder.

Moving Files and Folders

The File Shares Applet is designed for ease of use. There is more than one way to perform file transfers.

This section provides an example of a folder that is copied from a remote machine onto the local machine's desktop, deleted from the remote machine, and moved back from the local machine unto the remote machine, all from the File Shares Applet.

Step 1 Launch the File Shares Applet by clicking on a bookmark in the Virtual Office portal.

Step 2 Double-click the **C:** drive, double-click the **Documents and Settings** folder, then double-click a specific folder, for example, the one that holds the **Desktop** folder.

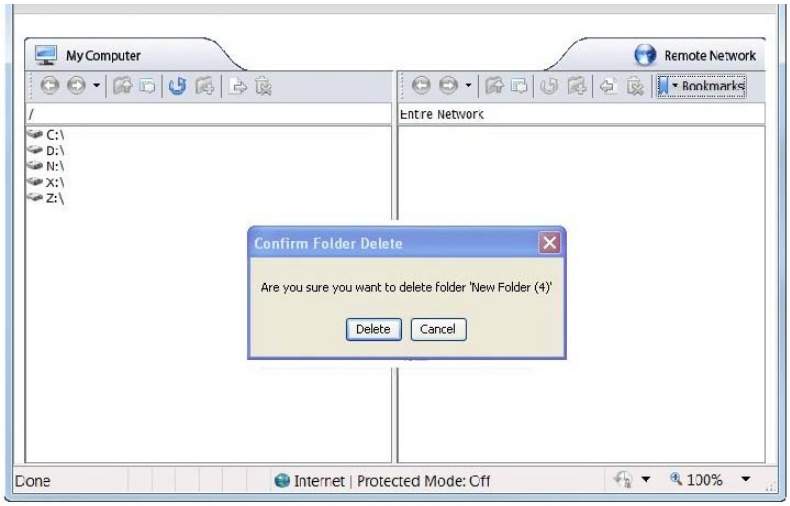
Step 3 The current directory shows the **Desktop** folder. Select a file or folder from the remote machine and drag its icon onto the **Desktop** folder in the local machine. This will copy the item from the remote machine directly onto the desktop.

Step 4 Once the transfer is complete, double-click on the **Desktop** folder. The folder copied from the remote machine will display in that folder.

Note The item still exists on the remote machine. To initiate a move, not a copy, you must use the **Move** command from the right-click menu.

Step 5 To delete the original file or folder, select it by clicking on it once, and press the **Delete** button on the tool bar. Alternatively, the item can be deleted by using the right-click menu. The File Shares Applet displays a delete confirmation window. Click the **Delete** button in the pop-up to delete the item.

Warning **The File Shares Applet will completely delete the file or folder from the remote machine. In the case of a folder, nested items will also be deleted. These items will not be sent to the recycle bin on either machine and are not recoverable.**



Step 6 Once the file or folder has been deleted, the File Shares Applet will automatically refresh, removing the item from the current directory. To copy it from the local machine back to the remote machine, click-and-drag like in **Step 2**, or use the **Copy** icon from the local machine's tool bar.

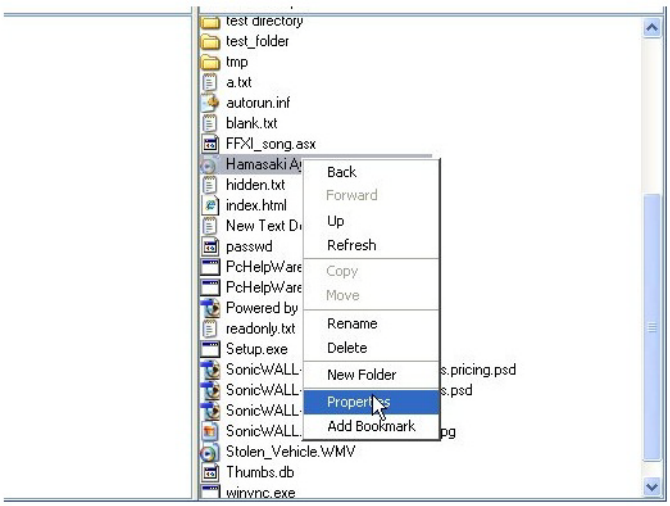
Note The **Copy** icon in the toolbar automatically moves the selected file to whatever directory is currently open. To move an item to a different folder, either drag-and-drop it into the desired destination or open the desired destination prior to clicking **Copy**.

Launching a File Directly from the File Shares Applet

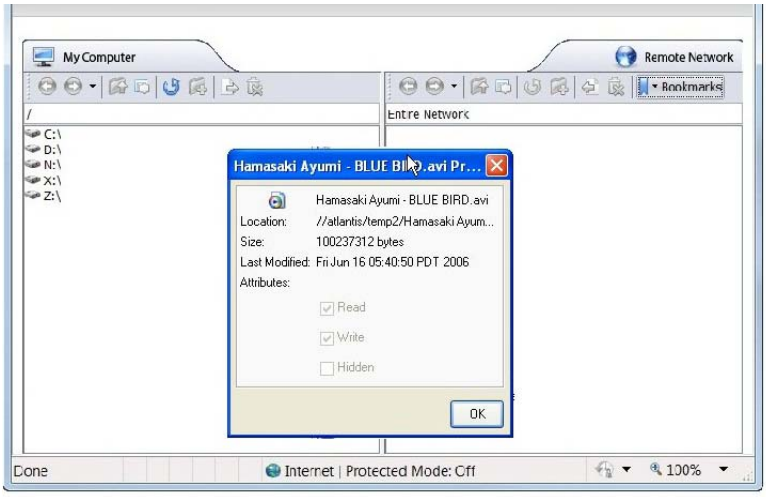
Files can be launched from within the File Shares Applet. This section provides an example where a remote file is queried for its properties, bookmarked and opened.

Step 1 Launch the File Shares Applet by clicking on a bookmark in the Virtual Office portal.

Step 2 Right click the file and select **Properties**.



The file's properties will be displayed in a separate window.



Step 3 To open the file, double-click on the file. Alternatively, create a bookmark to it, and launch the file from the bookmark menu. To create a bookmark, select the **Add Bookmark** option from the right-click menu. The name of the file is the default name of the new bookmark, but a new name can be entered if so desired.

Step 4 Then select the bookmark, either from the portal or from the bookmark tab in the toolbar.

Note Files launched from within the File Shares Applet must be downloaded to the local machine before they can be opened. The File Shares Applet will store the file in a temporary directory while it is being used. The File Shares Applet will also try to delete the file after use, but may be unable to do so depending on whether or not another program is accessing it. Use caution when opening files with sensitive material.

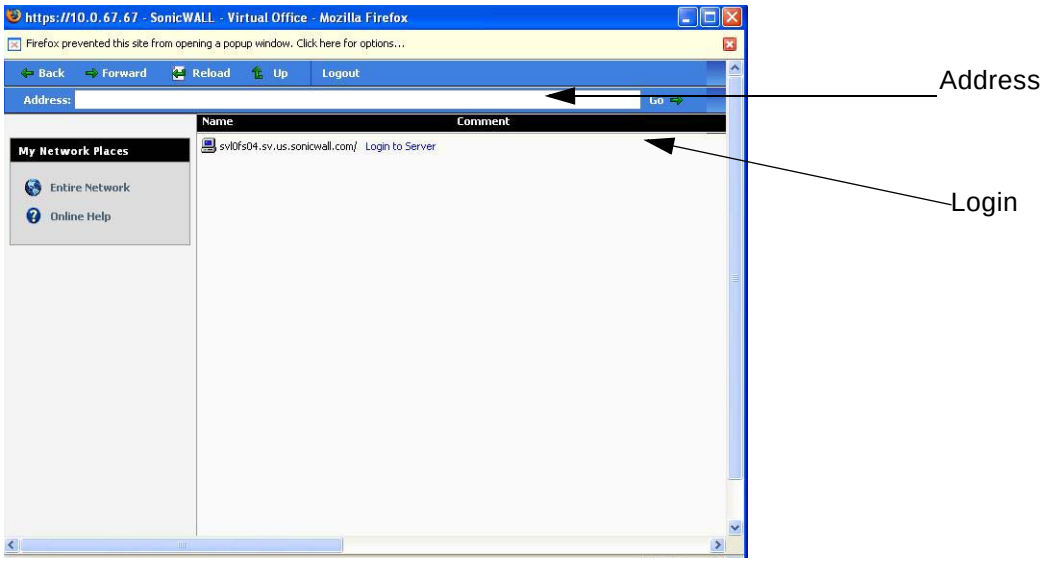
Using HTML-Based File Shares

File shares provide remote users with a secure Web interface to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.

Note The server can be specified either by name or by IP address, for example, **\\moosedc** or **\\10.50.165.2**. For names to work, it is necessary that DNS and/or WINS be properly configured by the administrator on the SRA appliance to be able to resolve host names.

To create a file share, perform the following steps:

Step 1 Click on the **File Shares** button. Virtual Office displays a dialog box that provides a hot link to a login prompt.



Note Pop-up window blockers may prevent File Shares from functioning properly. Configure your browser to allow pop-up windows on the SSL VPN portal site.

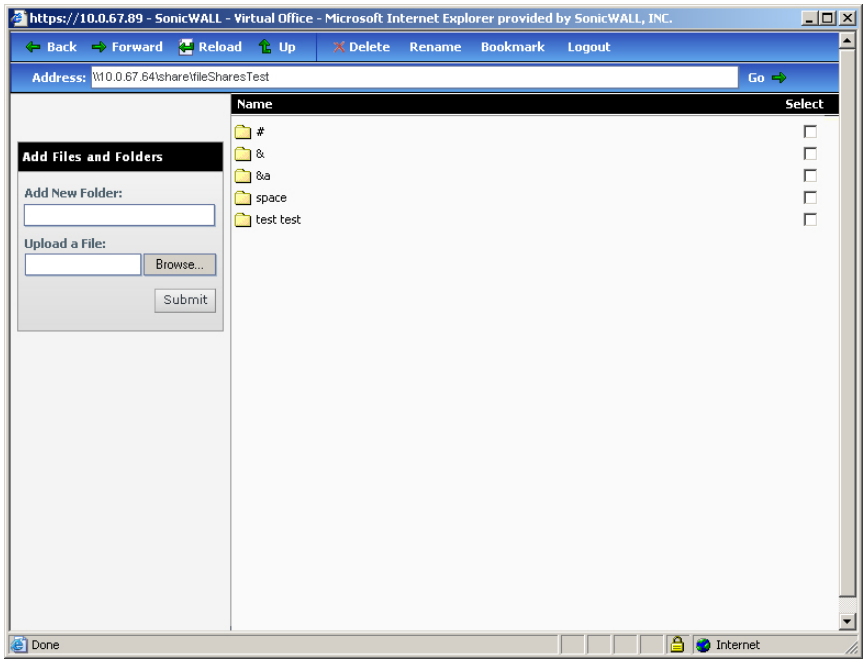
Step 2 To specify a new share path (as an example, **\\moosedc**) in the **Address** field. You need to precede the share name with two back slashes. For example: **\\file-directory01.example.com**.

Step 3 To connect to a pre-existing file share, click the **Login to Server** link next to the file share name.

Step 4 Click the **go** prompt to display the **Enter Network Password** dialog box.

Step 5 Type a valid username in the User Name field and a valid password in the Password field and click **Login**.

Step 6 Virtual Office displays the home File Share screen that you have specified, displaying folders on the network to which you can navigate.



The following table describes the controls at the top of the File Share window.

Table 2 File Share Controls

Button	Description
Back	Navigate to the previous File Share location.
Forward	Navigates forward to the previous File Share location after you have pressed the **Back** button.
Reload	Reloads the current folder to display any changes.
Up	Navigates
Delete	Deletes the selected folder or folders. Note that only empty folders can be deleted. If there are files in the folder, an error message is displayed. Delete all files out of the folder and then delete the folder.
Rename	Renames the selected folders and files. Select items by checking the check box next to their name under the **Select** column.
Bookmark	Creates a new bookmark to the current File Share location.
Logout	Logout of the File Share service.

Step 7 You can now navigate the folders and files in the File Share as you would through Windows Explorer or other file management systems.

Step 8 To add a new folder in the current File Share location, type the name of the folder in the **Add New Folder:** field and click **Submit**.

Step 9 To add a file in the current File Share location, click the **Browse...** button. Navigate to the location of the file on your computer in the **Choose file** window that opens, select the file and click **OK**, and then click **Submit** in the File Share window.

Managing Bookmarks

Bookmarks are objects that enable you to connect to a location or application conveniently and quickly. The Virtual Office Bookmark system allows bookmarks to be created at the group and user levels. The administrator can create both group and user bookmarks which will apply to applicable users while individual users can create only personal (user-level) bookmarks.

Since bookmarks are stored within the security appliance's local configuration files, it is necessary for group and user bookmarks to be correlated to defined group and user entities. When working with local groups and users (LocalDomain), this is automated since the administrator must manually define the groups and users on the device. Similarly, when working with external groups (not LocalDomain), the correlation is automated since creating an external domain creates a corresponding local group.

However, when working with external users, a local user entity must exist so that any user-created (personal) bookmarks can be stored within the SRA appliance's configuration files. The need to store bookmarks on the SRA appliance itself is because LDAP, RADIUS, and NT authentication external domains do not provide a direct facility to store such information as bookmarks.

Rather than requiring administrators to manually create local users for external domain users wishing to use personal bookmarks, Dell SonicWALL SSL VPN automatically creates a corresponding local user entity when an external domain user logs in to the Virtual Office.

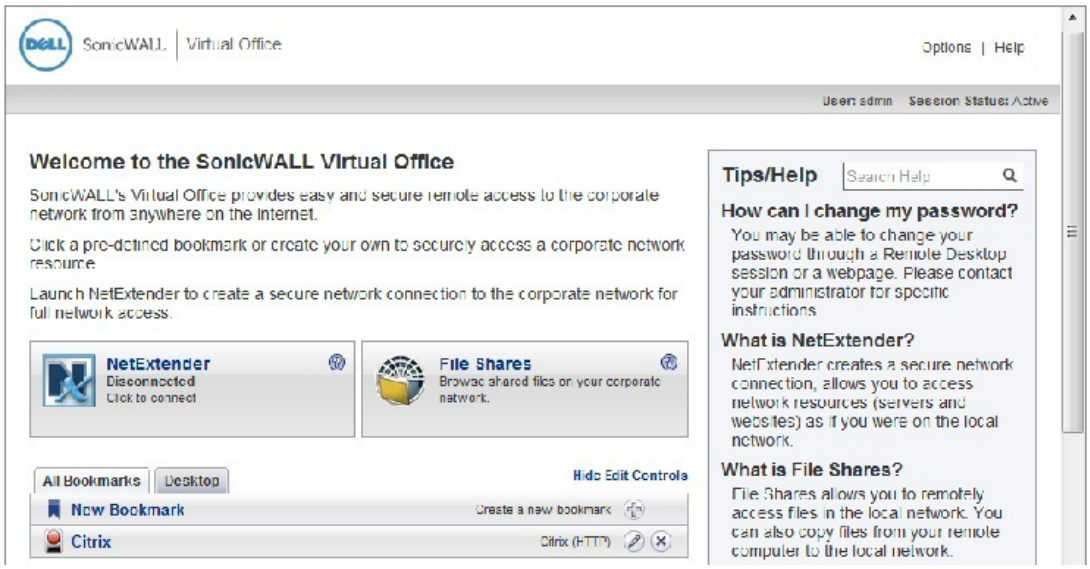
The following sections describe basic bookmark tasks:

- “Adding Bookmarks” section on page 133
- “Editing Bookmarks” section on page 138
- “Removing Bookmarks” section on page 139
- “Using Bookmarks” section on page 139

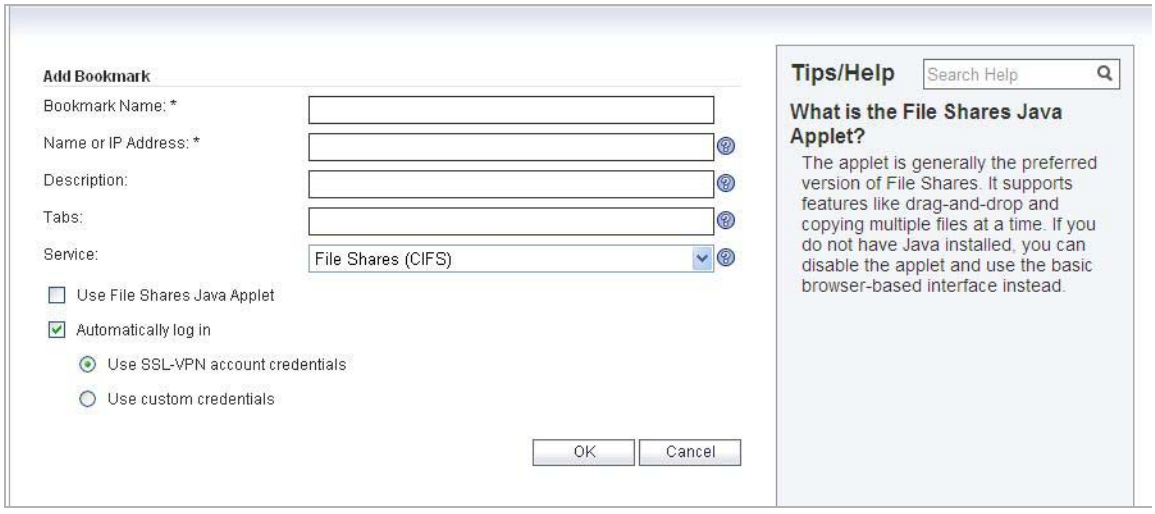
Adding Bookmarks

Bookmarks provide a convenient way for you to access Web, FTP, or other services on the remote network that you will connect to frequently. To define bookmarks, perform the following:

Step 1 In the Virtual Office window at the top of the bookmarks table, click **Show Edit Controls** and then click **Create a new bookmark**.


SonicWALL | Virtual Office
Options | Help
User: admin Session Status: Active
Welcome to the SonicWALL Virtual Office
SonicWALL's Virtual Office provides easy and secure remote access to the corporate network from anywhere on the Internet.
Click a pre-defined bookmark or create your own to securely access a corporate network resource.
Launch NetExtender to create a secure network connection to the corporate network for full network access.
NetExtender
Disconnected
Click to connect
File Shares
Browse shared files on your corporate network.
All Bookmarks
Desktop
Hide Edit Controls
New Bookmark
Create a new bookmark
Citrix
Citrix (HTTP)
Tips/Help
Search Help
How can I change my password?
You may be able to change your password through a Remote Desktop session or a webpage. Please contact your administrator for specific instructions.
What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local network.
What is File Shares?
File Shares allows you to remotely access files in the local network. You can also copy files from your remote computer to the local network.

Step 2 In the Add Bookmark screen, enter a descriptive name in the **Bookmark Name** field.


Add Bookmark
Bookmark Name: *
Name or IP Address: *
Description:
Tabs:
Service:
File Shares (CIFS)
Use File Shares Java Applet
Automatically log in
Use SSL-VPN account credentials
Use custom credentials
OK
Cancel
Tips/Help
Search Help
What is the File Shares Java Applet?
The applet is generally the preferred version of File Shares. It supports features like drag-and-drop and copying multiple files at a time. If you do not have Java installed, you can disable the applet and use the basic browser-based interface instead.

Step 3 Enter the domain name, IP address, or IPv6 address of a host machine on the LAN in the **Name or IP Address** field. IPv6 addresses should be enclosed in brackets (i.e. the [and] symbols). You may also enter the wildcard variable **%USERNAME%** to display the current user name. Variables are case-sensitive.

Step 4 In the **Description** field, optionally enter a friendly description to be displayed in the bookmark table.

Step 5 Select the user permissions level from the **Allow user to edit/delete** drop-down list. You can select **Use user policy**, **Allow**, or **Deny**.

Step 6 Select the service type in the **Service** drop-down list. You can select from the following services:

- Terminal Services (RDP - ActiveX)
- Terminal Services (RDP - Java)
- Virtual Network Computing (VNC)
- Citrix Portal (Citrix)
- Web (HTTP)
- Secure Web (HTTPS)
- External Web Site
- File Shares (CIFS)
- File Transfer Protocol (FTP)
- Telnet
- Secure Shell version 1 (SSHv1)
- Secure Shell version 2 (SSHv2)

The following sections provide additional details about adding the different types of bookmarks:

- "Citrix Bookmarks" on page 134
- "RDP ActiveX and Java Bookmarks" on page 135
- "Web Bookmarks" on page 137
- "FTP Bookmarks" on page 138
- "SSHv2 Bookmarks" on page 138

Once the configuration has been updated, the new bookmark will be displayed in the Virtual Office Bookmarks table. Click on a bookmark description to go to the bookmark location that you have defined.

Citrix Bookmarks

For Citrix bookmarks, you can select the following options:

- Designate that it be a secure Citrix connection by selecting the **HTTPS Mode** check box.
- Select **Always use Java in Internet Explorer** to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ActiveX client or plugin must be used with IE. This setting lets users avoid installing a Citrix client or plugin specifically for IE browsers. Java is used with Citrix by default on other browsers and also works with IE. Enabling this check box leverages this portability.
- Select **Always use specified Citrix ICA Server** to explicitly specify the Citrix ICA Server Address for the Citrix ICA Session. By default, the Bookmark uses the information provided in the ICA configuration on the Citrix server.

RDP ActiveX and Java Bookmarks

ActiveX and Java RDP bookmarks offer several features that are not available in other bookmarks.

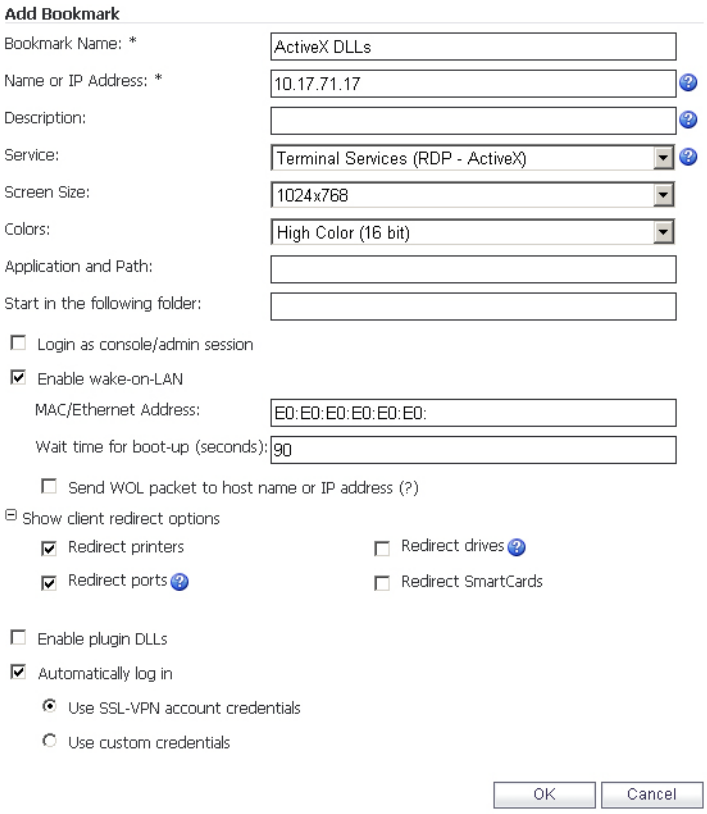
Tip The ActiveX client is only supported on the Internet Explorer browser, while the Java client is supported on all platforms and browsers that are compatible with Dell SonicWALL SSL VPN.

Step 1 Enter the desired **Bookmark Name**.

Step 2 Enter the **Name or IP Address** of the resource you are trying to reach. You can also use an IPv6 address.

Step 3 Select **Terminal Services (RDP - ActiveX)** or **Terminal Services (RDP -Java)** from the **Services** list.

Step 4 Continue to configure the RDP ActiveX or Java Bookmark as follows:



Option	Usage
Screen Size	Select the default screen size to be used when users execute this bookmark. It is advised that you select a size equal to or smaller than your current desktop screen size. ActiveX RDP bookmarks also have a **full-screen** option that will display the RDP window in full screen mode. To toggle from the RDP window back to your desktop, press **Alt-Tab**.
Colors	Select the default color depth to be used when users execute this bookmark.
Application and Path	To have the RDP session launch an application when the bookmark is initiated, enter the path to the application in the **Application and Path (optional):** field. For example, **C:\Program Files\Example\app.exe** (optional).
Start in the following folder	Enter the local folder to execute application commands in (optional).
Login as console/admin session	Check this option to enable console and admin commands on login.
Enable Wake on LAN	Select this option to send WoL packets to the host. This option also allows entering one or more **Mac Address**es (separated by spaces) for the machines to wake and the desired **Wait time for boot up** before cancelling the WoL operation. To send the WoL packet to the hostname or IP of this bookmark, check the **Send WOL packet to bookmark host Name or IP address** check box, this option can be applied in tandem with a Mac address.
Redirects (ActiveX only)	Optionally expand **Show windows advanced options** and select any of the redirect check boxes **Redirect printers**, **Redirect drives**, **Redirect ports**, or **Redirect SmartCards** to redirect those devices on the local network for use in this bookmark session.
Redirects (Java only)	Optionally expand **Show windows advanced options** and select any of the redirect check boxes **Redirect printers**, **Redirect drives**, **Redirect ports**, **Redirect SmartCards**, **Redirect clipboard** and **Redirect plug and play devices**, as well as any of the following additional features for use in this bookmark session: **Display connection bar**, **Auto reconnection**, **Desktop background**, **Window drag**, **Menu/ window animation**, **Themes**, or **Bitmap caching**. If the client application will actually be RDP 6 (Java), you can select any of the following options as well: **Dual monitors**, **Font smoothing**, **Desktop composition**, and **Remote Application**.
Automatically log in	Check this option and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark.

Tip The ActiveX client is only supported on the Internet Explorer browser, while the Java client is supported on all platforms and browsers that are compatible with Dell SonicWALL SSL VPN.

Step 5 When you are finished. Click the **Add** button to add this bookmark to your Virtual Office list.

Determining the Remote Computer's Full Name or IP Address

Complete the following steps to determine the full name of the computer to which the RDP bookmark is pointing:

Step 1 Right click on the **My Computer** icon on the desktop of the remote computer, and select **Properties**.

Step 2 Click the **Remote** tab.

Step 3 The full computer name will be listed under Remote Desktop.

Complete the following steps to determine the IP address of your computer.

Step 1 In the Windows **Start** menu on the remote computer, navigate to **Run...**

Step 2 Type **cmd** to open the command interpreter and click **OK**.

Step 3 Type **ipconfig**. The IP address of your computer is displayed.

Configuring Remote Desktop Access on the Remote Computer

Complete the following steps to allow remote desktop access to the computer that is the target of the RDP bookmark:

Step 1 Right click on the **My Computer** icon on the desktop, and select **Properties**.

Step 2 Click the **Remote** tab.

Step 3 Under Remote Desktop, select the check box for **Allow users to connect remotely to this computer**.

Step 4 Click **OK**.

Web Bookmarks

For HTTP(S) bookmarks, you can select **Use SSL-VPN account credentials to log in** or configure custom credentials for use with Single Sign-On. To disable the use of SSO, clear the **Automatically log in** check box. Select the Forms-based Authentication check box to use this method, and then fill in the following fields that are exposed:

- Configure the **User Form Field** to be the same as the 'name' or 'id' attribute of the HTML element representing User Name in the Login form, for example:
  <input type=text name='userid'>
- Configure the **Password Form Field** to be the same as the 'name' or 'id' attribute of the HTML element representing Password in the Login form, for example:
  <input type=password name='PASSWORD' id='PASSWORD' maxlength=128>

For External Web Site bookmarks, select **HTTPS Mode** to encrypt Web communication with SSL. External Web Site bookmarks are used to access an offloaded Web site or portal using a bookmark. Select **Disable security warning** if you do not want a security warning dialog box

to be displayed when a user clicks this bookmark. If left unchecked, the warning dialog will allow the user to select a “Do not show this warning again” option if the user has permissions to edit this bookmark (set above).

You are about to be redirected to a Web site that may not be secure. Do you want to continue?
Do not show this warning again?
Yes
Cancel

For more information about offloaded applications, see the Application Offloading section in the *Dell SonicWALL SSL VPN Administrator’s Guide*.

FTP Bookmarks

For FTP bookmarks, click **Show advance server configuration** to select the character encoding. You can also select **Use SSL-VPN account credentials to log in** or configure custom credentials for use with Single Sign-On. To disable the use of SSO, clear the **Automatically log in** check box.

SSHv2 Bookmarks

For SSHv2 bookmarks, you must have SUN JRE 1.6.0_10 or higher and must be connecting to a server that supports SSHv2. There are also options to **Automatically accept host key** and to **Bypass username**. The bypass option should only be used for SSHv2 servers that do not require authentication in the initial connection session (such as Dell SonicWALL security appliances).

Editing Bookmarks

You can change the IP address, domain name, or IPv6 address as well as the service and other settings associated with an existing bookmark.

Note Only user-created Bookmarks can be edited or deleted by the user. Global or Group Bookmarks pre-defined by the administrator cannot be edited or deleted.

To edit a bookmark to change its name or associated IP address, perform the following steps:

Step 1 Identify a bookmark in the Virtual Office Bookmarks list for which you want to change an IP address or domain name or other settings.

Step 2 In the Virtual Office Bookmarks list, click on the Configure icon for an existing bookmark. The **Edit Bookmark** dialog box displays.

Step 3 To change the bookmark name, domain name or IP address of the bookmark, edit the names in the **Bookmark Name** or **Name or IP Address** fields.

Step 4 To change the service, select a new **Service** from the drop-down menu.

Step 5 Optionally change other settings specific to the **Service** type.

Step 6 Optionally enable or disable the **Automatically log in** setting, or change the credentials selection.

Step 7 Click **Apply**. The Virtual Office home page displays with the new IP address or domain name.

Removing Bookmarks

To remove a bookmark, perform the following steps:

Step 1 Identify a bookmark in the Virtual Office Bookmarks list that you want to remove.

Step 2 In the Virtual Office Bookmarks list, click on the delete icon for the bookmark you want to remove. The bookmark disappears from the list.

Using Bookmarks

The following sections describe how to use the various types of bookmarks:

- "Using Remote Desktop Bookmarks" section on page 139
- "Using VNC Bookmarks" section on page 141
- "Using FTP Bookmarks" section on page 144
- "Using Telnet Bookmarks" section on page 147
- "Using SSHv1 Bookmarks" section on page 147
- "Using SSHv2 Bookmarks" section on page 148
- "Using Web Bookmarks" section on page 149
- "Using File Share Bookmarks" section on page 149
- "Using Citrix Bookmarks" section on page 150
- "Global Bookmark Single Sign-On Options" section on page 155
- "Per-Bookmark Single Sign-On Options" section on page 155

Using Remote Desktop Bookmarks

Remote Desktop Protocol (RDP) bookmarks enable you to establish remote connections with a specified desktop. Dell SonicWALL SSL VPN supports the RDP5 standard with both Java and ActiveX clients. RDP5 ActiveX can only be used through Internet Explorer, while RDP5 Java can be run on any platform and browser supported by the Dell SonicWALL SSL VPN. The basic functionality of the two clients is the same; however, the Java client is a native RDP client and supports the following features that the ActiveX client does not:

- Redirect clipboard
- Redirect plug and play devices
- Display connection bar
- Auto reconnection
- Desktop background
- Window drag
- Menu/window animation
- Themes
- Bitmap caching

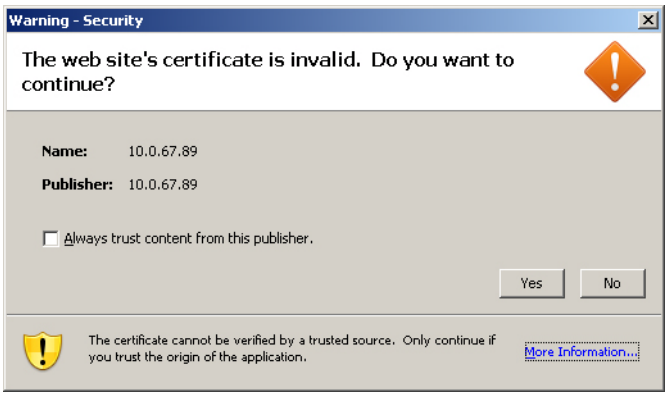
If the Java client application is RDP 6, it also supports:

- Dual monitors
- Font smoothing
- Desktop composition

Note RDP bookmarks can use a port designation if the service is not running on the default port.

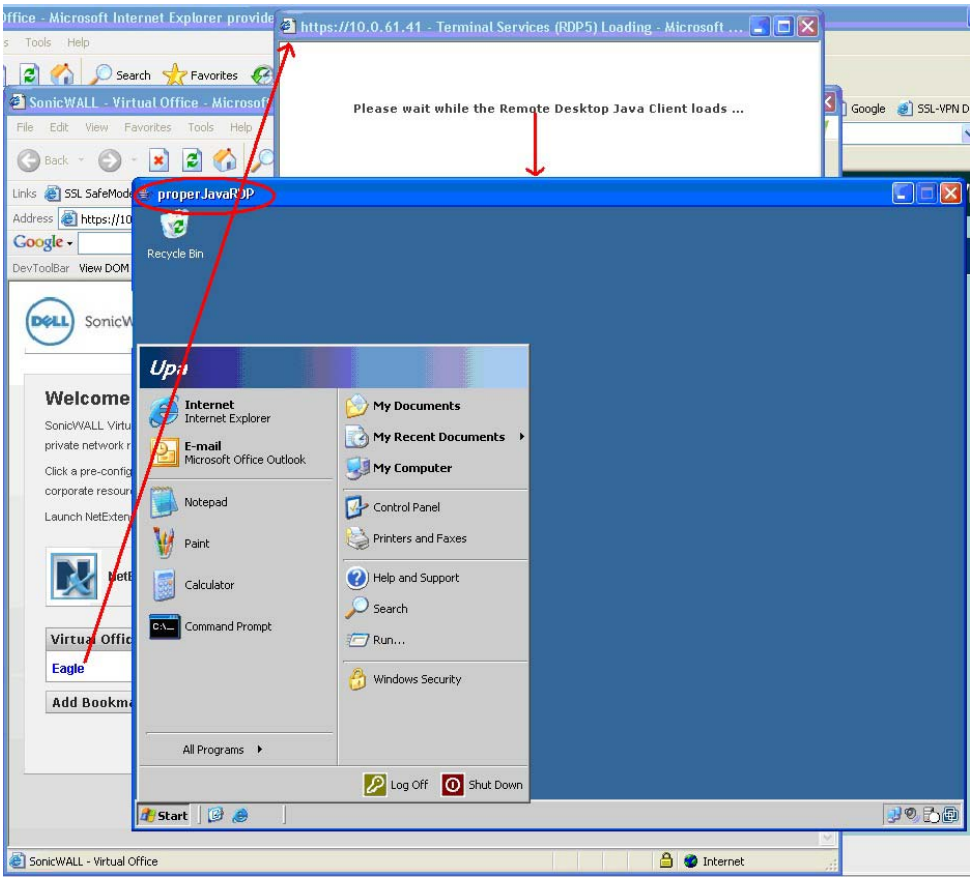
Tip To terminate your remote desktop session, be sure to log off from the Terminal Server session. If you wish to suspend the Terminal Server session (so that it can be resumed later) you may simply close the remote desktop window.

Step 1 Click on the **RDP** bookmark. Continue through any warning screens that display by clicking **Yes** or **Ok**.


Warning - Security
The web site's certificate is invalid. Do you want to continue?
Name: 10.0.67.89
Publisher: 10.0.67.89
Always trust content from this publisher.
Yes
No
The certificate cannot be verified by a trusted source. Only continue if you trust the origin of the application.
More Information...

Step 2 Enter your username and password at the login screen and select the proper domain name from the drop-down menu.

Step 3 A window is displayed indicating that the Remote Desktop Client is loading. The remote desktop then loads in its own windows. You can now access all of the applications and files on the remote computer.

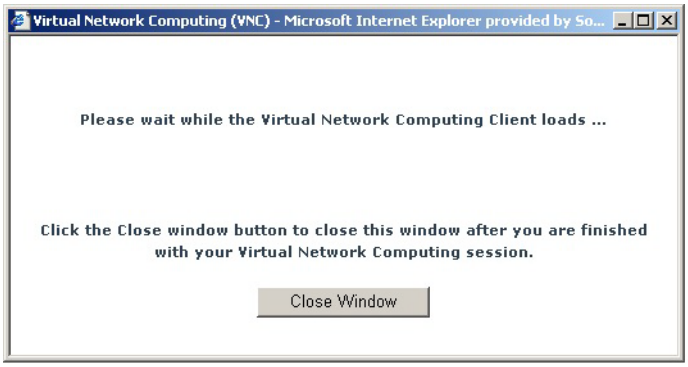


For information on configuring options for RDP bookmarks, see “RDP ActiveX and Java Bookmarks” on page 135.

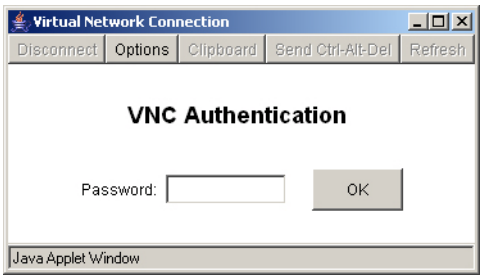
Using VNC Bookmarks

Step 1 Click the VNC bookmark. The following window is displayed while the VNC client is loading.

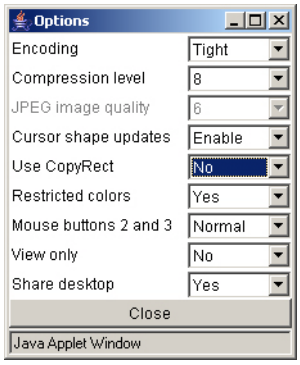
Note VNC can have a port designation if the service is running on a different port.


Virtual Network Computing (VNC) - Microsoft Internet Explorer provided by So...
Please wait while the Virtual Network Computing Client loads ...
Click the Close window button to close this window after you are finished with your Virtual Network Computing session.
Close Window

Step 2 When the VNC client has loaded, you will be prompted to enter your password in the **VNC Authentication** window.



Step 3 To configure VNC options, click the **Options** button. The **Options** window is displayed.



The following table describes the options that can be configured for VNC.

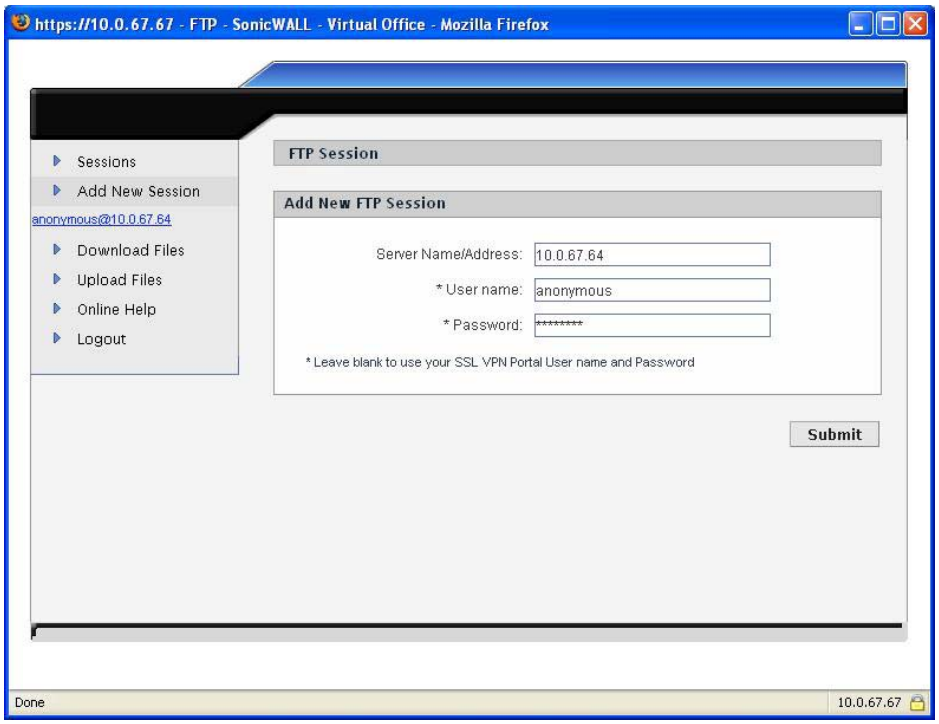
Table 3 VNC Options

Option	Default	Description of Options
Encoding	Tight	**Hextile** is a good choice for fast networks, while **Tight** is better suited for low-bandwidth connections. From the other side, the **Tight** decoder in TightVNC Java viewer is more efficient than **Hextile** decoder so this default setting can also be acceptable for fast networks.
Compression Level	Default	Use specified compression level for **Tight** and **Zlib** encodings. Level 1 uses minimum of CPU time on the server but achieves weak compression ratios. Level 9 offers best compression but may be slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over higher-speed networks. The **Default** value means that the server's default compression level should be used.
JPEG image quality	6	This cannot be modified.
Cursor shape updates	Enable	Cursor shape updates is a protocol extension used to handle remote cursor movements locally on the client side, saving bandwidth and eliminating delays in mouse pointer movement. Note that current implementation of cursor shape updates does not allow a client to track mouse cursor position at the server side. This means that clients would not see mouse cursor movements if the mouse was moved either locally on the server, or by another remote VNC client. Set this parameter to **Disable** if you always want to see real cursor position on the remote side. Setting this option to **Ignore** is similar to **Enable** but the remote cursor will not be visible at all. This can be a reasonable setting if you don't care about cursor shape and don't want to see two mouse cursors, one above another.
Use CopyRect	Yes	CopyRect saves bandwidth and drawing time when parts of the remote screen are moving around. Most likely, you don't want to change this setting.
Restricted colors	No	If set to **No**, then 24-bit color format is used to represent pixel data. If set to **Yes**, then only 8 bits are used to represent each pixel. 8-bit color format can save bandwidth, but colors may look very inaccurate.
Mouse buttons 2 and 3	Normal	If set to **Reversed**, the right mouse button (button 2) will act as if it was the middle mouse button (button 3), and vice versa.
View only	No	If set to **Yes**, then all keyboard and mouse events in the desktop window will be silently ignored and will not be passed to the remote side.
Share desktop	Yes	If set to **Yes**, then the desktop can be shared between clients. If this option is set to **No** then an existing user session will end when a new user accesses the desktop.

Using FTP Bookmarks

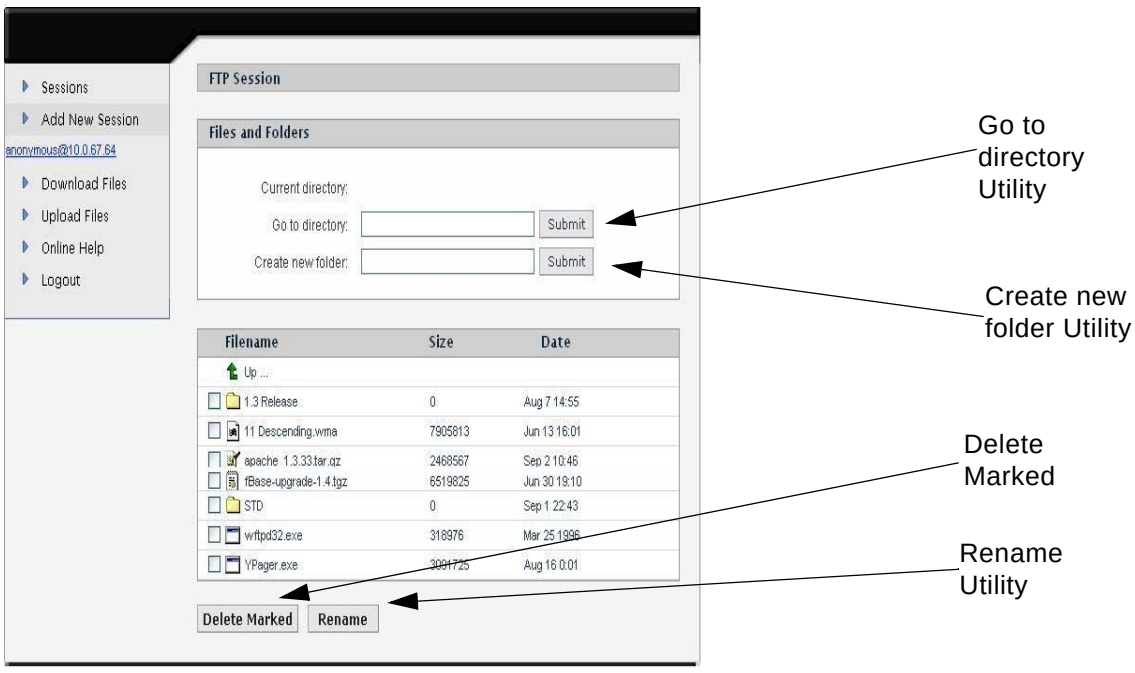
FTP bookmarks can use a port designation if the service is not running on the default port.

Step 1 Click the **FTP** bookmark. The **FTP Session** dialog box displays.



Step 2 Enter your username and password. If you want to use your Virtual Office username and password, simply leave the fields blank.

Step 3 Click **Submit**. An FTP session displays.



Step 4 You can use the following utilities in the FTP site:

- To manually navigate to a folder, enter the folder name in the **Go to directory** field and click **Submit**.
- To create new folders in the directory, use the **Create new folder** fields.
- To delete multiple files, click in the check boxes of files or folders you want to remove and click **Delete Marked**.
- To rename a file or folder, click in the check box of a file or a folder and click **Rename**.

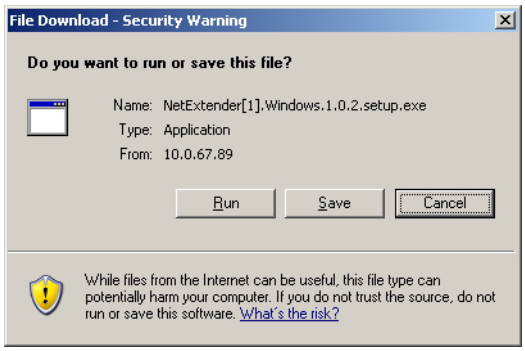
Step 5 To initiate another FTP session, click the **Add New Session** button. To return to the initial FTP session, click the link for it (in the form username@ipaddress) under the **Add New Session** button.

Downloading Files

To download a file, perform the following:

Step 1 Click **Download Files** in the navigation bar.

Step 2 Click on the name of the file in the **Filename** column. The File Download window displays.

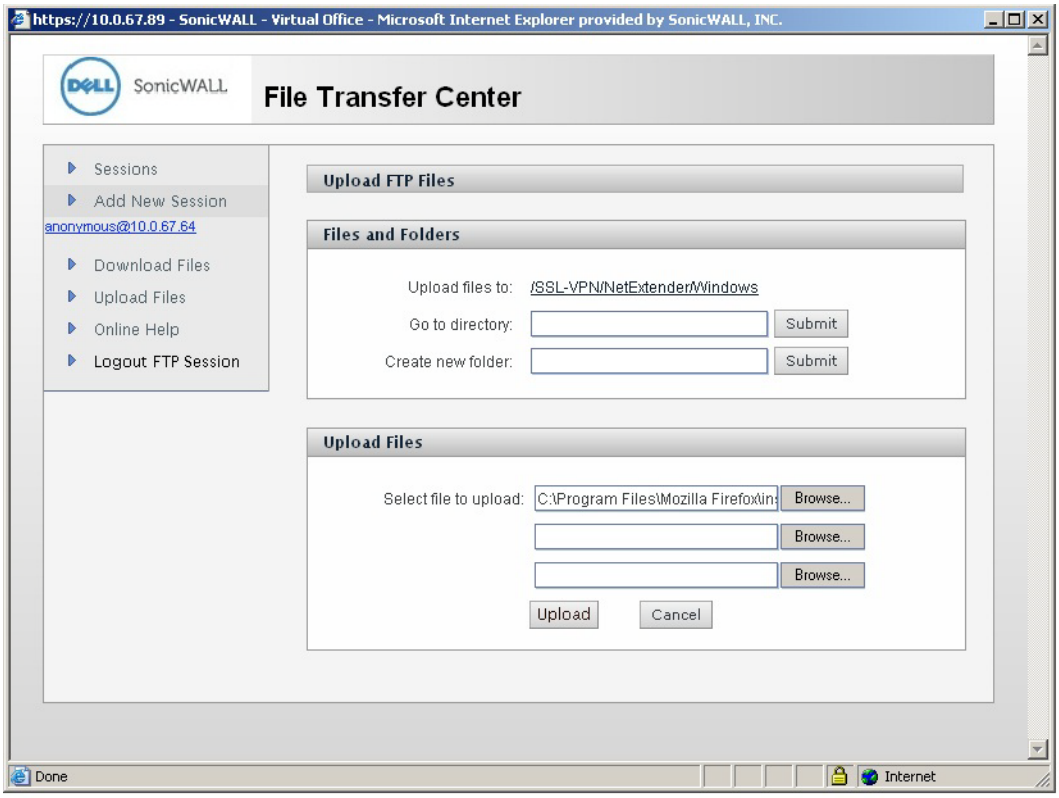

File Download - Security Warning
Do you want to run or save this file?
Name: NetExtender[1].Windows.1.0.2.setup.exe
Type: Application
From: 10.0.67.89
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Step 3 Click **Run** to launch the file. Click **Save** to save it to your computer.

Uploading Files

To upload a file, perform the following:

Step 1 Click **Upload Files** in the navigation bar. The Upload FTP Files window will be displayed.



Step 2 The current directory is displayed in the **Upload files to:** field. To navigate to a different directory, enter the directory name in the **Go to directory:** field. To create a new folder in the current directory, enter the name of the folder in the **Create new folder:** field and click submit.

Step 3 Select the file you want to upload by clicking the **Browse...** button and navigating to the file. You can upload up to three files at once.

To navigate between uploads, click the **Sessions** link.

Step 4 Click **Upload** to upload the files.

Using Telnet Bookmarks

Step 1 Click on the Telnet bookmark.

Telnet bookmarks can use a port designation for servers not running on the default port.

Step 2 Click **OK** to any warning messages that are displayed. A Java-based Telnet window launches.

Step 3 If the device you are Telnetting to is configured for authentication, enter your username and password.

Using SSHv1 Bookmarks

SSH bookmarks can use a port designation for servers not running on the default port.

Step 1 Click on the SSHv1 bookmark. A Java-based SSH window is launched.

Step 2 Enter your username and password.

Step 3 A SSH session is launched in the Java applet.

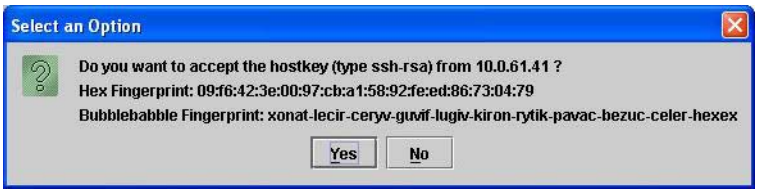
Tip Some versions of the JRE may cause the SSH authentication window to pop up behind the SSH window.

Using SSHv2 Bookmarks

SSH bookmarks can use a port designation for servers not running on the default port.

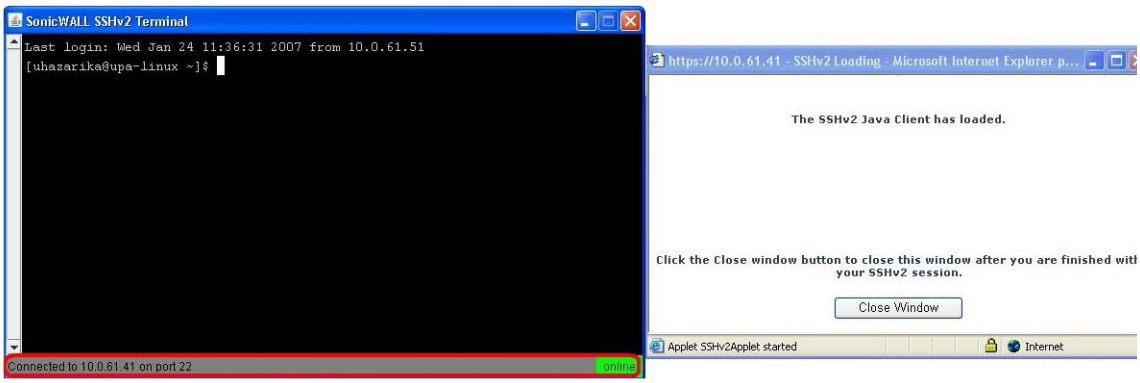
Step 1 Click on the SSHv2 bookmark. A Java-based SSH window displays. Type your user name in the **Username** field and click **Login**.

Step 2 A hostkey popup displays. Click **Yes** to accept and proceed with the login process.



Step 3 Enter your password and click **OK**.

Step 4 The SSH terminal launches in a new screen.


SonicWALL SSHv2 Terminal
Last login: Wed Jan 24 11:36:31 2007 from 10.0.61.51
[uhazarika@upa-linux ~]$
Connected to 10.0.61.41 on port 22
online
https://10.0.61.41 - SSHv2 Loading - Microsoft Internet Explorer p...
The SSHv2 Java Client has loaded.
Click the Close window button to close this window after you are finished with your SSHv2 session.
Close Window
Applet SSHv2Applet started
Internet

Using Web Bookmarks

Step 1 Click on the HTTP or HTTPS bookmark.

Note HTTP bookmarks can have a port designation and a path.

Step 2 A new window is launched in your default browser that connects to the domain name or IP address specified in the bookmark.

HTTP & HTTPS Bookmarks have been tested and verified to support the following web applications:

- Microsoft Outlook Web Access 2010, Outlook Web Access 2007, and Outlook Web Access 2003.
- Windows Sharepoint 2007, Windows Sharepoint Services 3.0 and Windows Sharepoint Services 2.0.
- Please note the client integrated features of Sharepoint are not supported.
- Lotus Domino Web Access 7.0
- Novell Groupwise Web Access 7.0

Other applications may work but there may be problems accessing pages that are malformed, have advanced HTML features, use an unsupported authentication method (for example, Windows Integrated Authentication) and URLs that are embedded in Macromedia Flash, Java or ActiveX. If a web application does not work with a HTTP or HTTPS Bookmark, contact your administrator.

Using File Share Bookmarks

For information on using File Share bookmarks, see the "Using HTML-Based File Shares" section on page 130.

Using Citrix Bookmarks

Citrix is a remote access, application sharing service, similar to RDP. It enables users to remotely access files and applications on a central computer over a secure connection. There are two types of Citrix bookmarks:

- “ActiveX Citrix Bookmark” on page 150
- “Java Citrix Bookmark” on page 153

ActiveX Citrix Bookmark

When using the Internet Explorer web browser, Citrix bookmarks launch the ActiveX Citrix client. The following steps describe how to launch and use the ActiveX Citrix client.

Step 1 Click on the Citrix bookmark. The first time you use a Citrix bookmark, it will install the Citrix Web Client on your computer if you do not already have it.

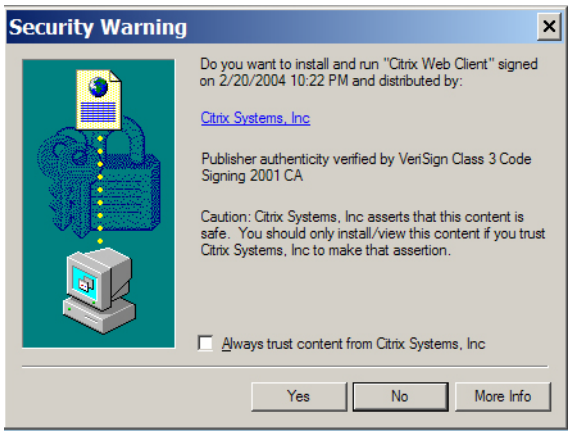
Step 2 Click **Install** to install the client.

Internet Explorer - Security Warning
Do you want to install this software?
Name: Citrix Web Client
Publisher: Citrix Systems, Inc
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

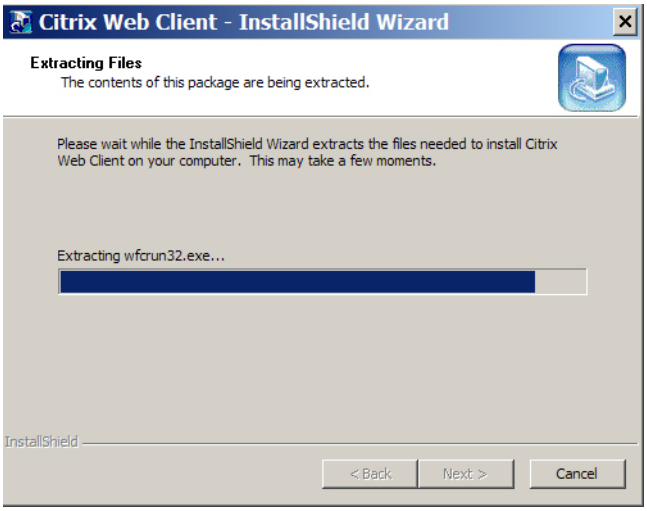
Step 3 The Citrix Web Client begins to install. If prompted, click the banner to grant ActiveX control to the Citrix Web Client.

https://10.0.61.150 - Citrix Installation - Microsoft Internet Explorer
This site might require the following ActiveX control: 'Citrix Web Client' from 'Citrix Systems, Inc'. Click here to install...
Please wait while the Citrix Web Client is installed ...
After installation, you will be automatically redirected to the Citrix portal

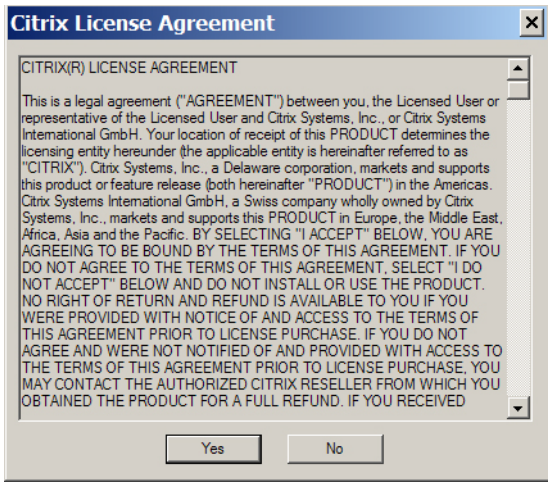
Step 4 Click **Yes** to the Security Warning message that is displayed.


Security Warning
Do you want to install and run "Citrix Web Client" signed on 2/20/2004 10:22 PM and distributed by:
Citrix Systems, Inc
Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA
Caution: Citrix Systems, Inc asserts that this content is safe. You should only install/view this content if you trust Citrix Systems, Inc to make that assertion.
Always trust content from Citrix Systems, Inc
Yes
No
More Info

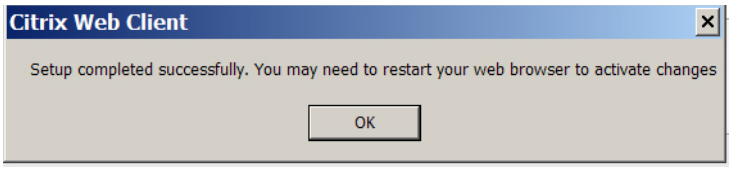
Step 5 The Citrix Web Client installs.


Citrix Web Client - InstallShield Wizard
Extracting Files
The contents of this package are being extracted.
Please wait while the InstallShield Wizard extracts the files needed to install Citrix Web Client on your computer. This may take a few moments.
Extracting wfcrun32.exe...
InstallShield
< Back
Next >
Cancel

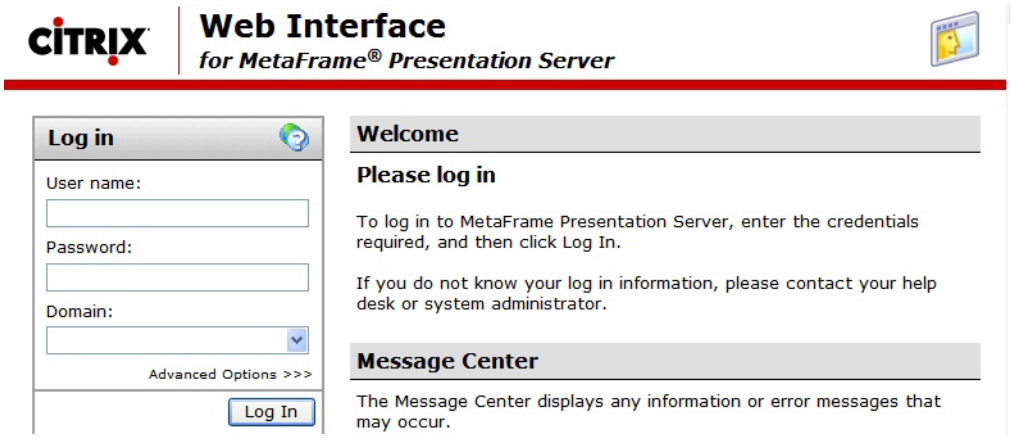
Step 6 Click **Yes** to the Citrix license agreement.


Citrix License Agreement
CITRIX(R) LICENSE AGREEMENT
This is a legal agreement ("AGREEMENT") between you, the Licensed User or representative of the Licensed User and Citrix Systems, Inc., or Citrix Systems International GmbH. Your location of receipt of this PRODUCT determines the licensing entity hereunder (the applicable entity is hereinafter referred to as "CITRIX"). Citrix Systems, Inc., a Delaware corporation, markets and supports this product or feature release (both hereinafter "PRODUCT") in the Americas. Citrix Systems International GmbH, a Swiss company wholly owned by Citrix Systems, Inc., markets and supports this PRODUCT in Europe, the Middle East, Africa, Asia and the Pacific. BY SELECTING "I ACCEPT" BELOW, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, SELECT "I DO NOT ACCEPT" BELOW AND DO NOT INSTALL OR USE THE PRODUCT. NO RIGHT OF RETURN AND REFUND IS AVAILABLE TO YOU IF YOU WERE PROVIDED WITH NOTICE OF AND ACCESS TO THE TERMS OF THIS AGREEMENT PRIOR TO LICENSE PURCHASE. IF YOU DO NOT AGREE AND WERE NOT NOTIFIED OF AND PROVIDED WITH ACCESS TO THE TERMS OF THIS AGREEMENT PRIOR TO LICENSE PURCHASE, YOU MAY CONTACT THE AUTHORIZED CITRIX RESELLER FROM WHICH YOU OBTAINED THE PRODUCT FOR A FULL REFUND. IF YOU RECEIVED
Yes
No

Step 7 When the Citrix Web Client has installed, click **OK** If the Citrix Web Interface login window does not display, restart your Web browser and launch the Citrix bookmark again.

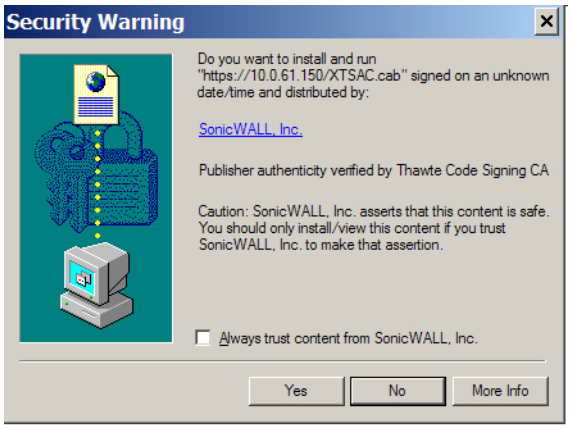


Step 8 Enter your username, password, and domain in the Citrix Web Interface login window.


CITRIX
Web Interface
for MetaFrame® Presentation Server
Log in
User name:
Password:
Domain:
Advanced Options >>>
Log In
Welcome
Please log in
To log in to MetaFrame Presentation Server, enter the credentials required, and then click Log In.
If you do not know your log in information, please contact your help desk or system administrator.
Message Center
The Message Center displays any information or error messages that may occur.

Step 9 The Citrix Web Interface home page is displayed. Click on the application you want to use.

Step 10 You may be prompted to install additional Citrix software.


Security Warning
Do you want to install and run "https://10.0.61.150/XTSAC.cab" signed on an unknown date/time and distributed by:
SonicWALL, Inc.
Publisher authenticity verified by Thawte Code Signing CA
Caution: SonicWALL, Inc. asserts that this content is safe. You should only install/view this content if you trust SonicWALL, Inc. to make that assertion.
Always trust content from SonicWALL, Inc.
Yes
No
More Info

Step 11 The shared application is now launched.

Java Citrix Bookmark

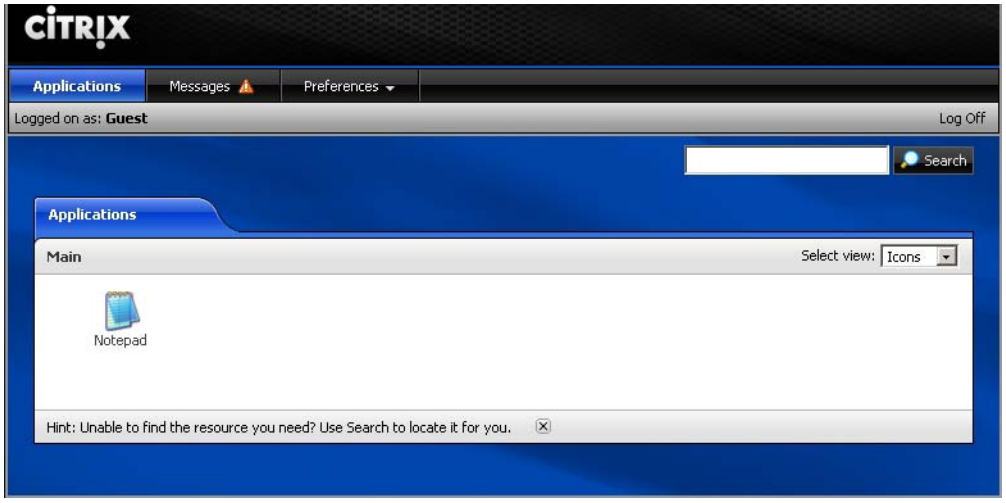
When using a non-Internet Explorer web browser, Citrix bookmarks launch the Java Citrix client. The following steps describe how to launch and use the Java Citrix client.

Step 1 Click on the Citrix bookmark. The login window displays.

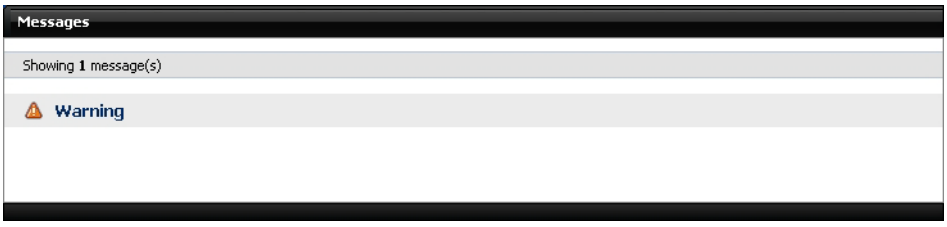
Step 2 For **Logon type**, select either **Anonymous** or **Explicit**. Select Anonymous to login without providing a user name. Note that you may not be able to access resources that require authentication. Select Explicit to login with a user name and password. You may also be required to provide a domain name or NDS context.

Welcome
To log on, select an authentication method, enter the required information, and then click Log On.
If you do not know your logon details, contact your system administrator.
Logon type:
Explicit
User name:
userisusing
Password:
Log On

Step 3 Click the **Log On** button. The Citrix Java applet displays. The default applications will display in the Applications section in the middle of the window.

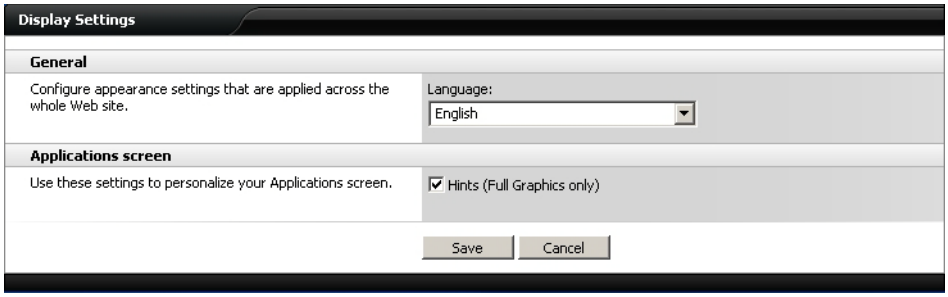


Step 4 Click on **Messages** to view any Citrix messages you have received.

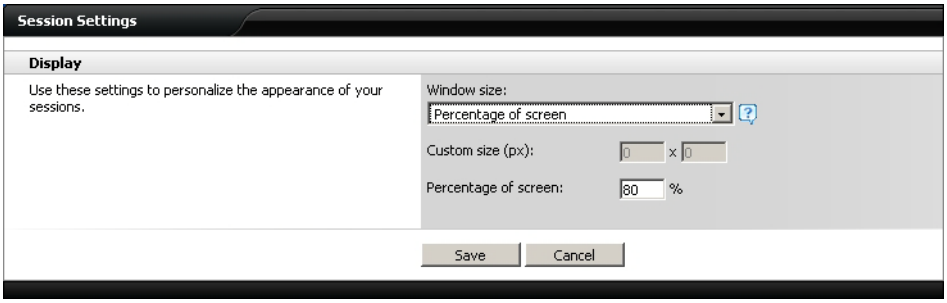


Step 5 Click on **Preferences** to customize the Citrix Java applet settings.

Step 6 Select **Display Settings** to change the language and to specify if Citrix hints should be displayed.



Step 7 Select **Session Settings** to customize the default window size for Citrix sessions.



Step 8 In the **Window Size** drop-down menu, select one of the following options:

- **No preference**: Uses the default setting configured by your administrator.
- **Full screen**: Resources are maximized to fill your screen.
- **Seamless**: Resources that support resizing appear in resizable windows.
- **Custom dimensions**: Enables you to specify the width and height of the resource window in pixels.
- **Percentage of screen**: Enables you to specify the percentage of your screen the resources will occupy.

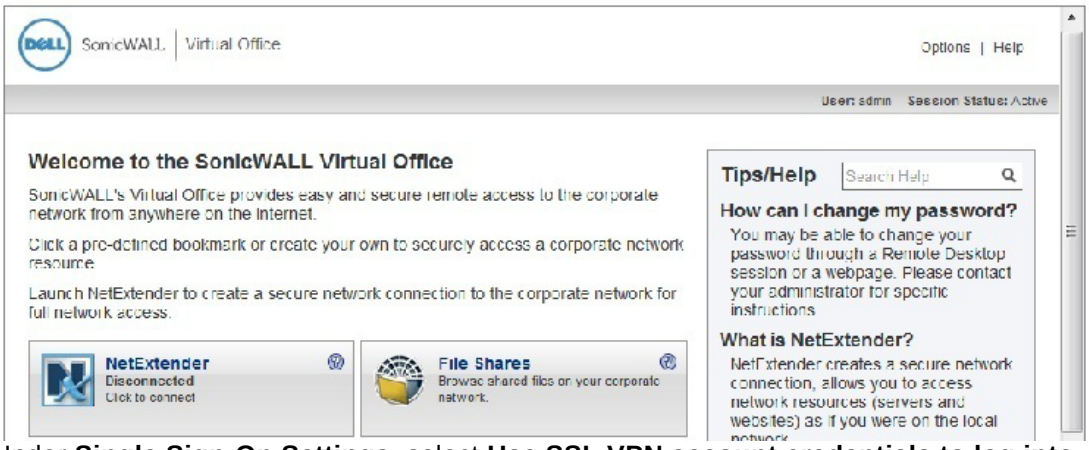
Step 9 Select **Account Settings** to configure the behavior of your sessions when you log out.

Step 10 Select the **Log off all sessions** check box to shut down all of your active resources when you log off from the Citrix session. If you disable this check box, any active resources that are hosted on a remote server continue to run when you log off. (Offline applications always continue to run when you log off from the Citrix session.)

Global Bookmark Single Sign-On Options

You can configure single sign-on using the **Options** button on the main Virtual Office page. SSO settings will be enabled only if the administrator has configured user- controlled single sign-on (SSO). To configure SSO bookmark options, perform the following tasks:

Step 1 Click the **Options** button at the top right of the Virtual Office. The **User Options** page displays.


SonicWALL | Virtual Office
Options | Help
User: admin Session Status: Active
Welcome to the SonicWALL Virtual Office
SonicWALL's Virtual Office provides easy and secure remote access to the corporate network from anywhere on the Internet.
Click a pre-defined bookmark or create your own to securely access a corporate network resource.
Launch NetExtender to create a secure network connection to the corporate network for full network access.
NetExtender
Disconnected
Click to connect
File Shares
Browse shared files on your corporate network.
Tips/Help
Search Help
How can I change my password?
You may be able to change your password through a Remote Desktop session or a webpage. Please contact your administrator for specific instructions.
What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local

Step 2 Under **Single Sign-On Settings**, select **Use SSL VPN account credentials to log into bookmarks** to enable SSO for bookmarks. Leave the box unchecked if you do not want to use SSO for bookmarks.

Step 3 Click **Save** to save your changes.

Fileshares will use the configured domain name of which the user is a member to supply to the backend server. HTTP, HTTPS, FTP, RDP - ActiveX, RDP- Java will supply the username and password that was used to login. If the server is expecting a domain-prefixed username, SSO will fail. In some cases, a default domain can be specified at the server to allow SSO to succeed.

Per-Bookmark Single Sign-On Options

Dell SonicWALL SSL VPN supports per-bookmark single sign-on for the following bookmark services:

- Terminal Services (RDP - Active X)
- Terminal Services (RDP - Java)
- Web (HTTP)
- Secure Web (HTTPS)
- File Shares (CIFS)
- File Transfer Protocol (FTP)

Per-Bookmark SSO allows users to enable or disable SSO for individual bookmarks. This flexibility in specifying login credentials is useful in the following cases:

- Users who use multiple accounts to access a variety of resources.
- Users who use two-factor authentication to log in to the SSL VPN Virtual Office, but use a static password to access other resources.
- Users who need to access servers that require a domain prefix.

To configure per-bookmark SSO, perform the following tasks.

Step 1 Before enabling SSO on an individual bookmark, you must first enable SSO globally as described in the "Global Bookmark Single Sign-On Options" section on page 155.

Step 2 On the Virtual Office page, click on the **Create a new bookmark** button.

Step 3 Select one of the service types that supports per-bookmark SSO: **Terminal Services (RDP - Active X)**, **Terminal Services (RDP - Java)**, **Web (HTTP)**, **Secure Web (HTTPS)**, **File Shares (CIFS)**, or **File Transfer Protocol (FTP)**.

Step 4 To disable SSO for the bookmark, clear the **Automatically log in** check box.

Step 5 To use SSO for the bookmark, select the **Automatically log in** check box and then select one of the following radio buttons:

- **Use SSL-VPN account credentials** – allow login to the bookmark using the local user credentials configured on the SRA appliance
- **Use custom credentials** – allow login to the bookmark using the credentials you enter here; when selected, this option displays **Username**, **Password**, and **Domain** fields. Enter the custom credentials into the **Username**, **Password**, and **Domain** fields that are displayed.

  You can enter the custom credentials as text or use dynamic variables such as those shown below:

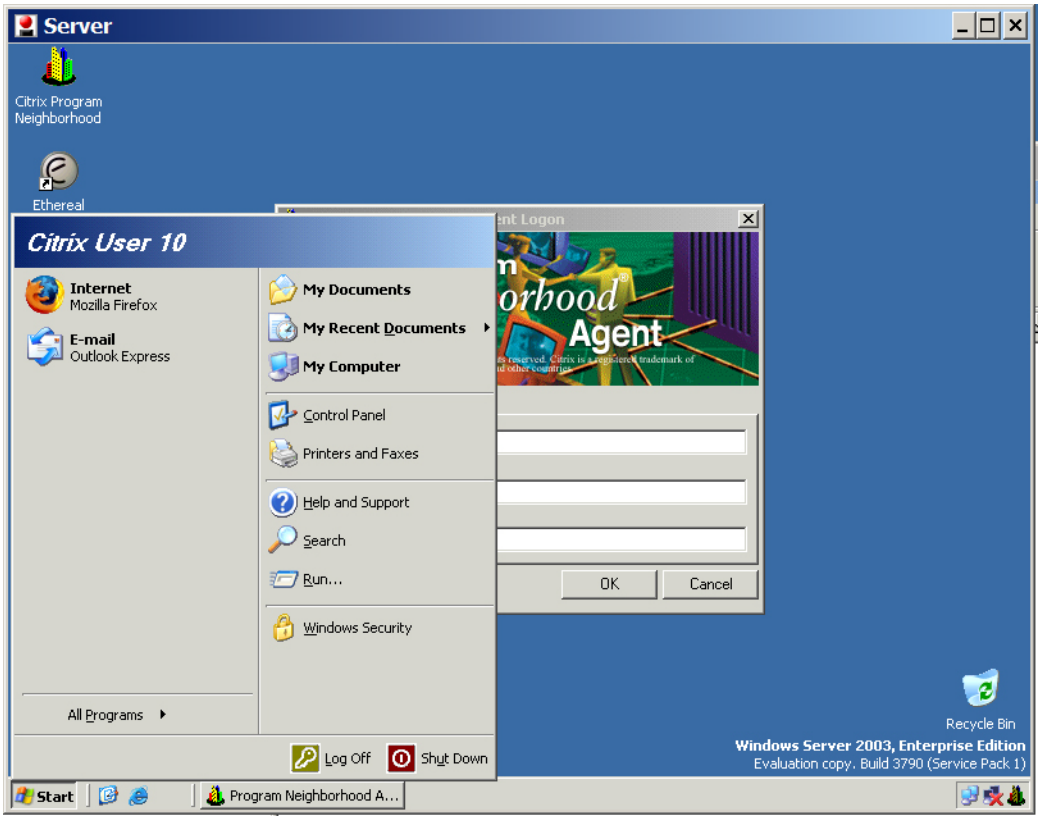
Text Usage	Variable	Example Usage
Login Name	%USERNAME%	US\%USERNAME%
Domain Name	%USERDOMAIN%	%USERDOMAIN\%USERNAME%
Group Name	%USERGROUP%	%USERGROUP%\%USERNAME%
Password	%PASSWORD%	%PASSWORD% or leave the field blank

Step 6 For Web (HTTP) and Secure Web (HTTPS) bookmarks, select the **Forms-based Authentication** check box to use this method for SSO, and then fill in the following fields that are exposed:

- Configure the **User Form Field** to be the same as the 'name' or 'id' attribute of the HTML element representing User Name in the Login form, for example:
  <input type=text name='userid'>
- Configure the **Password Form Field** to be the same as the 'name' or 'id' attribute of the HTML element representing Password in the Login form, for example:
  <input type=password name='PASSWORD' id='PASSWORD' maxlength=128>

Step 7 Click **OK**.

Step 8 Enter the **User name** and **password** for the service.



Logging Out of the Virtual Office

To end your session, simply return to the Virtual Office home page from wherever you are within the portal and click on the Logout button.

When using the Virtual Office with the **admin** username, the **Logout** button is not displayed. This is a security measure to ensure that administrators log out of the administrative interface, and not the Virtual Office.

Appendix A
Support Information

This appendix contains the following sections:

- "Contact Information" on page 159
- "GNU General Public License (GPL) Source Code" on page 159
- "Limited Hardware Warranty" on page 159
- "End User Licensing Agreement" on page 160

Contact Information

For timely resolution of technical support questions, visit Dell SonicWALL on the Internet at *<http://www.sonicwall.com/us/support.html>*. Web-based resources are available to help you resolve most technical issues or contact Dell SonicWALL Technical Support

Technical Support Contact Information:
Contact Support Page - http://www.sonicwall.com/us/support/contact.html
Contact SonicWALL Page - http://www.sonicwall.com/us/company/286.html

GNU General Public License (GPL) Source Code

Dell SonicWALL will provide a machine-readable copy of the GPL open source on a CD. To obtain a complete machine-readable copy, send your written request, along with a certified check or money order in the amount of US $25.00 payable to "Dell SonicWALL, Inc." to:

General Public License Source Code Request
Dell SonicWALL, Inc. Attn: Jennifer Anderson
2001 Logic Drive
San Jose, CA 95124-3452

Limited Hardware Warranty

All Dell SonicWALL appliances come with a 1-year Limited Hardware Warranty which provides delivery of critical replacement parts for defective parts under warranty. In addition, for 90 days from the warranty start date, Dell SonicWALL SRA 4600/1600 appliances are entitled to a Limited Software Warranty which provides bug fixes, updates and any maintenance releases that occur during the coverage term. Visit the Warranty Information page for details on your product's warranty:
http://www.sonicwall.com/us/support/Services.html#tab=warranty

Dell SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by Dell SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. Dell SonicWALL and its

suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At Dell SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. Dell SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of Dell SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of Dell SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. DELL SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL DELL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF DELL SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Dell SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

End User Licensing Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SONICWALL PRODUCT. BY INSTALLING OR USING THE SONICWALL PRODUCT, YOU (AS THE CUSTOMER, OR IF NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) INDICATE ACCEPTANCE OF AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT FOR AND ON BEHALF OF THE CUSTOMER. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, THEN DO NOT USE THE PRODUCT AND RETURN IT TO THE PLACE OF PURCHASE WITH PROOF OF PURCHASE WITHIN THIRTY (30) DAYS OF PURCHASE FOR A REFUND. IF YOU DO PROCEED TO INSTALL OR USE THE SONICWALL PRODUCT, YOU WILL HAVE INDICATED ACCEPTANCE AND AGREEMENT WITH THE TERMS AND CONDITIONS HEREIN. NOTWITHSTANDING THE FOREGOING, THIS AGREEMENT SHALL NOT SUPERSEDE ANY OTHER SIGNED AGREEMENT BETWEEN YOU AND SONICWALL THAT EXPRESSLY GOVERNS THE SONICWALL PRODUCT.

"Product" means the SonicWALL labeled hardware and related documentation ("Hardware") and/or proprietary SonicWALL labeled software, firmware and related documentation ("Software") purchased by the end user of the product either directly from SonicWALL or a Reseller (“Customer”). “Services” means the Support Services described below and any other services provided with or for the Products directly by SonicWALL or its agents. “Reseller” shall mean those entities to which SonicWALL or SonicWALL’s authorized distributors distribute the Products for resale to end users. Except as otherwise agreed upon by the parties, this Agreement will also cover any updates and upgrades to the Products provided to Customer by SonicWALL directly or through a Reseller (except as may be otherwise indicated, such updates and upgrades shall be deemed Products).

1. LICENSE(S) AND RESTRICTIONS

(a) Licenses. Subject to the terms and conditions of this Agreement, SonicWALL grants to Customer, and Customer accepts from SonicWALL, a nonexclusive, nontransferable (except as otherwise set forth herein) and nonsublicensable license (“License”) to:

(i) execute and use the Software on the Hardware with which the Software is provided (pre-installed) in accordance with the applicable Documentation; and,

(ii) for Software provided in standalone form (without Hardware), install, execute and use the Software on the Hardware or hardware device(s) on which it is intended to be used in accordance with the applicable Documentation and the License purchased. If Customer purchased multiple copies of standalone Software, Customer’s License to such standalone Software includes the right to install, use and execute up to the number of copies of Software Licenses purchased.

In addition, the License includes the right to (x) make a reasonable number of additional copies of the Software to be used solely for non-productive archival purposes, and (y) make and use copies of the end user documentation for Hardware and/or Software provided with the Products (“Documentation”) as reasonably necessary to support Customer’s authorized users in their use of the Products.

(b) License Limitations. Order acknowledgments, Documentation and/or the particular type of the Products/ Licenses purchased by Customer may specify limits on Customer’s use of the Software, and which limits apply to the License(s) granted hereunder for such Software. Such limits may consist of limiting the term of the License, or the number or amount of nodes, storage space, sessions, calls, users, subscribers, clusters, devices, ports, bandwidth, throughput or other elements, and/or require the purchase of separate Licenses to use or obtain particular features, functionalities, services, applications or other items. Use of the Software shall be subject to all such limitations.

(c) For Customer’s Internal Business. Each License shall be used by Customer solely to manage its own internal business operations as well as the business operations of its Affiliates. Notwithstanding the foregoing, if Customer is in the regular business of providing firewall, VPN or Security management for a fee to entities that are not its Affiliates (“MSP Customers”), Customer may use the Products for its MSP Customers provided that either (i) Customer, and not MSP Customers, maintain control and possession of the Products, or (ii) if MSP Customers have possession and/or control of Products in whole or in part, this Agreement must be provided to MSP Customers and they must agree that their use of the Products is subject to the terms and conditions of this Agreement. Customer agrees to indemnify and hold SonicWALL harmless from and against any claims by MSP Customers against SonicWALL relating to the Products and/or Customer’s services for MSP Customers. “Affiliate” means any legal entity controlling, controlled by, or under common control with a party to this Agreement, but only for so long as such control relationship exists.

(d) Evaluation License. If the Software is provided by SonicWALL or a Reseller at no charge for evaluation purposes, then Section 1(a) above shall not apply to such Software and instead Customer is granted a nonproduction License to use such Software and the associated documentation solely for Customer's own internal evaluation purposes for an evaluation period of up to thirty (30) days from the date of delivery of the Software, plus any extensions granted by SonicWALL in writing (the "Evaluation Period"). There is no fee for Customer's use of the Software for nonproduction evaluation purposes during the Evaluation Period, however, Customer is responsible for any applicable shipping charges or taxes which may be incurred, and any fees which may be associated with usage beyond the scope permitted herein. Notwithstanding anything otherwise set forth in this Agreement, Customer understands and agrees that evaluation Software is provided "AS IS" and that SonicWALL does not provide a warranty or maintenance services for evaluation Licenses.

(e) Restrictions. Customer may not (i) modify, translate, localize, adapt, rent, lease, loan, create or prepare derivative works of, or create a patent based on the Software or any part thereof, (ii) make copies except as expressly authorized under this Agreement, (iii) copy the Software onto any public or distributed network, (iv) modify or resell the Software, use the Software in connection with the operation of any nuclear facilities, or use for purposes which are competitive to SonicWALL, or (v) except as expressly authorized in Section 2(c) above, operate the Software for use in any time-sharing, outsourcing, service bureau or application service provider type environment. Unless and except to the extent authorized in the applicable Documentation, Software provided with and/or as the Product, in part or whole, is licensed for use only in accordance with the Documentation as part of the Product: Software components making up a Product may not be separated from, nor used on a separate or standalone basis from the Product. Each permitted copy of the Software and Documentation made by Customer hereunder must contain all titles, trademarks, copyrights and restricted rights notices as in the original. Customer understands and agrees that the Products may work in conjunction with third party products and Customer agrees to be responsible for ensuring that it is properly licensed to use such third party products. Any Software provided in object code form is licensed hereunder only in object code form. Except to the extent allowed by applicable law if located in the European Union, and then only with prior written notice to SonicWALL, Customer shall not disassemble or reverse engineer the Software in whole or in part or authorize others to do so. Customer agrees not to use the Software to perform comparisons or other "benchmarking" activities, either alone or in connection with any other software or service, without SonicWALL's written permission; or publish any such performance information or comparisons.

(f) Third Party Software. There may be certain third party owned software provided along with, or incorporated within, the Products ("Third Party Software"). Except as set forth below, such Third Party Software shall be considered Software governed by the terms and conditions of this Agreement. However, some Products may contain other Third Party Software that is provided with a separate license agreement, in which case such Third Party Software will be governed exclusively by such separate license agreement ("Third Party License") and not this Agreement. Any such Third Party Software that is governed by a Third Party License, and not this Agreement, will be identified on the applicable Product page on SonicWALL's website and/or in a file provided with the Product. Except as SonicWALL may otherwise inform Customer in writing, the Third Party License gives Customer at least the license rights granted above, and may provide additional license rights as to the Third Party Software, but only with respect to the particular Third Party Software to which the Third Party License applies. SUCH THIRD PARTY SOFTWARE UNDER A THIRD PARTY LICENSE IS PROVIDED WITHOUT ANY WARRANTY FROM SONICWALL AND ITS SUPPLIERS, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. Notwithstanding the foregoing, SonicWALL shall honor its warranty, maintenance and support obligations in respect to the SonicWALL Products regardless of whether the warranty, maintenance or support issue is caused in whole or in part by the Third Party Software provided by SonicWALL with the Product.

(g) Updates/Upgrades. If Customer purchases or otherwise is eligible to receive a SOFTWARE update or upgrade, you must be properly licensed to use the Product identified by SonicWALL as being eligible for the update/ upgrade in order to install and use the SOFTWARE update/ upgrade. A SOFTWARE update/ upgrade replaces and/or supplements the Software Product that formed the basis for your eligibility for the update/upgrade, and does not provide you an additional License (copy) of the Software to use separately from the Software Product to be updated/ upgraded. You may use the resulting updated/upgraded Product only in accordance with the terms of this Agreement.

(h) Activation Keys May Expire. Certain Products, including Security Services that provide regular ongoing updates for Software (e.g., Security Service consisting of anti-virus signature updates), may come with an activation key or license key (a key that must be entered to activate the Product, “Activation Key”). If the Activation Key for a Product is not activated within five (5) years from the date of issuance by SonicWALL, such Activation Key(s) may expire and no longer activate the Product. Products that come with an expiring Activation Key will operate for the contracted term of the License (or purchased Security Service), so long as the Activation Key is activated within five (5) years from SonicWALL’s date of issuance.

2. OWNERSHIP

SonicWALL and its licensors are the sole and exclusive owners of the Software, and all underlying intellectual property rights in the Hardware. All rights not expressly granted to Customer are reserved by SonicWALL and its licensors.

3. TERMINATION OF LICENSE(S)

All licenses to the Software hereunder shall terminate if Customer fails to comply with any of the provisions of this Agreement and does not remedy such breach within thirty (30) days after receiving written notice from SonicWALL. Customer agrees upon termination to immediately cease using the Software and to destroy all copies of the Software which may have been provided or created hereunder.

4. SUPPORT SERVICES

SonicWALL’s current Support Service offerings (“Support Services”) and the terms and conditions applicable to such Support Services are set forth in SonicWALL’s Support Services Terms located http://www.sonicwall.com/us/support/ Services.html and are incorporated herein by reference. Support Services may require an additional fee. Unless otherwise agreed to in writing, SonicWALL’s Support Services are subject to SonicWALL’s Support Services Terms which are in effect at the time the Support Services are purchased by Customer, and these terms and conditions will be incorporated herein by reference at that time. SonicWALL reserves the right to change the Support Services Terms from time to time by posting such changes on its website, which shall apply to any Support Services purchased on or after the date of such posting.

5. SONICWALL WARRANTY

(a) Warranty. SonicWALL warrants to Customer (original purchaser Customer only) that for the applicable warranty period (“Warranty Period”) the Hardware will be free from any material defects in materials or workmanship and the Software, if any, will substantially conform to the Documentation applicable to the Software and the License purchased (“Limited Warranty”). Except as may indicated otherwise in writing by SonicWALL, the Warranty Period for Hardware is one year from the date of registration of the Hardware Product (or if sooner, seven days after initial delivery of the Hardware Product to Customer), and the applicable warranty period for

Software is ninety days from the date of registration of the Software Product (or if sooner, seven days after initial delivery/download) of the Software Product to/by Customer. SonicWALL does not warrant that use of the Product(s) will be uninterrupted or error free nor that SonicWALL will correct all errors. The Limited Warranty shall not apply to any non-conformance (i) that SonicWALL cannot recreate after exercising commercially reasonable efforts to attempt to do so; (ii) caused by misuse of the Product or by using the Product in a manner that is inconsistent with this Agreement or the Documentation; (iii) arising from the modification of the Products by anyone other than SonicWALL; or (iv) caused by any problem or error in third party software or hardware not provided by SonicWALL with the Product regardless of whether or not the SonicWALL Product is designed to operate with such third party software or hardware. SonicWALL's sole obligation and Customer's sole and exclusive remedy under any express or implied warranties hereunder shall be for SonicWALL to use commercially reasonable efforts to provide error corrections and/or, if applicable, repair or replace parts in accordance with SonicWALL's Support Services Terms. Customer shall have no rights or remedies under this Limited Warranty unless SonicWALL receives Customer's detailed written warranty claim within the applicable warranty period.

(b) Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH ABOVE, TO MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW SONICWALL HEREBY DISCLAIMS ON BEHALF OF ITSELF, ITS SUPPLIERS, DISTRIBUTORS AND RESELLERS ALL WARRANTIES, EXPRESS, STATUTORY AND IMPLIED, APPLICABLE TO THE PRODUCTS, SERVICES AND/OR THE SUBJECT MATTER OF THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE.

6. LIMITATION OF LIABILITY

The Products are not designed, manufactured, authorized or warranted to be suitable for use in any system where a failure of such system could result in a situation that threatens the safety of human life, including without limitation any such medical, life support, aviation or nuclear applications. Any such use and subsequent liabilities that may arise from such use are totally the responsibility of Customer, and all liability of SonicWALL, whether in contract, tort (including without limitation negligence) or otherwise in relation to the same is excluded. Customer shall be responsible for mirroring its data, for backing it up frequently and regularly, and for taking all reasonable precautions to prevent data loss or corruption. SonicWALL shall not be responsible for any system downtime, loss or corruption of data or loss of production. NOTWITHSTANDING ANYTHING ELSE IN THIS AGREEMENT OR OTHERWISE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SONICWALL, ITS SUPPLIERS, DISTRIBUTORS OR RESELLERS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST OR CORRUPTED DATA, LOST PROFITS OR SAVINGS, LOSS OF BUSINESS OR OTHER ECONOMIC LOSS OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, ARISING OUT OF OR RELATED TO THIS AGREEMENT, THE PRODUCTS OR THE SERVICES, WHETHER OR NOT BASED ON TORT, CONTRACT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND WHETHER OR NOT SONICWALL HAS BEEN ADVISED OR KNEW OF THE POSSIBILITY OF SUCH DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, SONICWALL'S MAXIMUM LIABILITY TO CUSTOMER ARISING FROM OR RELATING TO THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNTS RECEIVED BY SONICWALL FOR THE PRODUCTS AND THE SERVICES PURCHASED BY CUSTOMER, PROVIDED THAT WHERE ANY CLAIM AGAINST SONICWALL RELATES TO PARTICULAR PRODUCT AND/OR SERVICES, SONICWALL'S MAXIMUM LIABILITY SHALL BE LIMITED TO THE AGGREGATE AMOUNT RECIEVED BY SONICWALL IN RESPECT OF THE PRODUCTS AND/OR SERVICES PURCHASED BY CUSTOMER AFFECTED BY THE MATTER GIVING RISE TO THE CLAIM. (FOR MAINTENANCE SERVICES OR A PRODUCT SUBJECT TO RECURRING FEES, THE LIABILITY SHALL NOT EXCEED THE AMOUNT RECEIVED BY

SONICWALL FOR SUCH MAINTENANCE SERVICE OR PRODUCT PURCHASED BY CUSTOMER DURING THE TWELVE (12) MONTHS PRECEDING THE CLAIM). CUSTOMER EXPRESSLY AGREES TO THE ALLOCATION OF LIABILITY SET FORTH IN THIS SECTION, AND ACKNOWLEDGES THAT WITHOUT ITS AGREEMENT TO THESE LIMITATIONS, THE PRICES CHARGED FOR THE PRODUCTS AND SERVICES WOULD BE HIGHER.

7. GOVERNMENT RESTRICTIONS

Customer agrees that it will not export or re-export the Products without SonicWALL's prior written consent, and then only in compliance with all requirements of applicable law, including but not limited to U.S. export control regulations. Customer has the responsibility to obtain any required licenses to export, reexport or import the Products. Customer shall defend, indemnify and hold SonicWALL and its suppliers harmless from any claims arising out of Customer’s violation of any export control laws relating to any exporting of the Products. By accepting this Agreement and receiving the Products, Customer confirms that it and its employees and agents who may access the Products are not listed on any governmental export exclusion lists and will not export or re-export the Products to any country embargoed by the U.S. or to any specially denied national (SDN) or denied entity identified by the U.S. Applicable export restrictions and exclusions are available at the official web site of the U.S. Department of Commerce Bureau of Industry and Security (www.bis.doc.gov). For purchase by U.S. governmental entities, the technical data and computer software in the Products are commercial technical data and commercial computer software as subject to FAR Sections 12.211, 12.212, 27.405-3 and DFARS Section 227.7202. The rights to use the Products and the underlying commercial technical date and computer software is limited to those rights customarily provided to the public purchasers as set forth in this Agreement. The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

8. GENERAL

a) Governing Law and Venue. This Agreement shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflict of laws principles that would require the application of laws of a different state. The parties agree that neither the United Nations Convention on Contracts for the International Sale of Goods, nor the Uniform Computer Information Transaction Act (UCITA) shall apply to this Agreement, regardless of the states in which the parties do business or are incorporated. Any action seeking enforcement of this Agreement or any provision hereof shall be brought exclusively in the state or federal courts located in the County of Santa Clara, State of California, United States of America. Each party hereby agrees to submit to the jurisdiction of such courts. Notwithstanding the foregoing, SonicWALL is entitled to seek immediate injunctive relief in any jurisdiction in the event of any alleged breach of Section 1 and/or to otherwise protect its intellectual property.

b) Assignment. Except as otherwise set forth herein, Customer shall not, in whole or part, assign or transfer any part of this Agreement or any rights hereunder without the prior written consent of SonicWALL. Any attempted transfer or assignment by Customer that is not permitted by this Agreement shall be null and void. Any transfer/assignment of a License that is permitted hereunder shall require the assignment/transfer of all copies of the applicable Software along with a copy of this Agreement, the assignee must agree to all terms and conditions of this Agreement as a condition of the assignment/transfer, and the License(s) held by the transferor Customer shall terminate upon any such transfer/assignment.

c) Severability. If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, such provision will be enforced to the maximum extent permissible and the remaining provisions of this Agreement will remain in full force and effect.

d) Privacy Policy. Customer hereby acknowledges and agrees that SonicWALL's performance of this Agreement may require SonicWALL to process or store personal data of Customer, its employees and Affiliates, and to transmit such data within SonicWALL or to SonicWALL Affiliates, partners and/or agents. Such processing, storage, and transmission may be used for the purpose of enabling SonicWALL to perform its obligations under this Agreement, and as described in SonicWALL's Privacy Policy (www.SonicWALL.com/us/Privacy_Policy.html, "Privacy Policy") and may take place in any of the countries in which SonicWALL and its Affiliates conduct business, including countries outside of the European Economic Area. SonicWALL reserves the right to change the Privacy Policy from time to time as described in the Privacy Policy.

e) Notices. All notices provided hereunder shall be in writing, delivered personally, or sent by internationally recognized express courier service (e.g., Federal Express), addressed to the legal department of the respective party or to such other address as may be specified in writing by either of the parties to the other in accordance with this Section.

f) Disclosure of Customer Status. SonicWALL may include Customer in its listing of customers and, upon written consent by Customer, announce Customer's selection of SonicWALL in its marketing communications.

g) Waiver. Performance of any obligation required by a party hereunder may be waived only by a written waiver signed by an authorized representative of the other party, which waiver shall be effective only with respect to the specific obligation described therein. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

h) Force Majeure. Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service as a result of causes beyond its reasonable control, and without its fault or negligence, including without limitation, acts of God, strikes, lockouts, riots, acts of war, epidemics, communication line failures, and power failures.

i) Audit. Customer shall maintain accurate records to verify compliance with this Agreement. Upon request by SonicWALL, Customer shall furnish (a copy of) such records to SonicWALL and certify its compliance with this Agreement.

j) Headings. Headings in this Agreement are for convenience only and do not affect the meaning or interpretation of this Agreement. This Agreement will not be construed either in favor of or against one party or the other, but rather in accordance with its fair meaning. When the term "including" is used in this Agreement it will be construed in each case to mean "including, but not limited to."

k) Entire Agreement. This Agreement is intended by the parties as a final expression of their agreement with respect to the subject matter hereof and may not be contradicted by evidence of any prior or contemporaneous agreement unless such agreement is signed by both parties. In the absence of such an agreement, this Agreement shall constitute the complete and exclusive statement of the terms and conditions and no extrinsic evidence whatsoever may be introduced in any judicial proceeding that may involve the Agreement. This Agreement represents the complete agreement and understanding of the parties with respect to the subject matter herein. This Agreement may be modified only through a written instrument signed by both parties.